

P-178

NASA Contractor Report 187042

# COLD-SAT Feasibility Study Safety Analysis

(NASA-CR-187042) COLD-SAT FEASIBILITY STUDY  
SAFETY ANALYSIS Final Report (Analex Corp.)  
178 p CSCL 229

N91-19157

Unclass  
63/18 0007513

Steven T. McHenry and James M. Yost  
*Analex Corporation*  
*Fairview Park, Ohio*

January 1991

Prepared for  
Lewis Research Center  
Under Contract NAS3-25515



National Aeronautics and  
Space Administration



## COLD-SAT FEASIBILITY STUDY SAFETY ANALYSIS

Steven T. McHenry and James M. Yost  
Analex Corporation  
Fairview Park, Ohio 44126

### ABSTRACT

The Cryogenic On-orbit Liquid Depot - Storage, Acquisition and Transfer (COLD-SAT) satellite presents some unique safety issues. The feasibility study conducted at the NASA Lewis Research Center desired a systems safety program that would be involved from the initial design in order to eliminate and/or control the inherent hazards. Because of this, a hazards analysis method was needed that: (1) identified issues that needed to be addressed for a feasibility assessment; and (2) identified all potential hazards that would need to be controlled and/or eliminated during the detailed design phases. This report presents the developed analysis method as well as the results generated for the COLD-SAT system.

## **I. Introduction/Unique Requirements**

The Cryogenic On-Orbit Liquid Storage, Acquisition, and Transfer (COLD-SAT) satellite presents some unique considerations from a safety perspective. NASA Lewis Research Center has conducted feasibility studies for this free-flying orbital experiment with a planned launch by an expendable launch vehicle (ELV) in 1998. The purpose of COLD-SAT is to perform subcritical liquid hydrogen ( $LH_2$ ) storage and transfer experiments under low-gravity conditions to provide engineering data for future space transportation missions. Gaseous hydrogen ( $GH_2$ ) and gaseous helium ( $GHe$ ) are also proposed for use in various components of the experiments.

Liquid hydrogen was chosen as the experimental fluid for two reasons. First, its use as the primary liquid rocket propellant makes it an obvious candidate (it has the highest specific impulse of current rocket fuels). Second, it will provide more restrictive (i.e. more conservative) data than other candidates, thereby making the experiment results broader and more applicable to other fluids.

In addition to the usual safety concerns involved with launching a space vehicle, COLD-SAT creates additional concerns due to its use of cryogenic hydrogen. Ground and launch operations are tremendously affected by this and will be modified in support of safety evaluations. The use of hydrazine ( $N_2H_4$ ), pyrotechnics, and pressure vessels on the spacecraft also provide the need for extensive safety input.

The approach used for this safety analysis is as follows. First, a hazard definition matrix was developed. Second, hazard definitions were defined in conjunction with this matrix. Next, each of the defined hazards was classified based on its applicability to the feasibility study. Finally, the hazards considered to be major concerns were evaluated by the system designers and safety engineers in order to identify proper design approaches and safety considerations. Each of these items will be discussed in detail in succeeding sections.

The intent of this analysis is to provide a baseline for the COLD-SAT program safety efforts. The structure of the analysis is such as to be very thorough, yet general in nature. Thus, the analysis can be viewed as a complete analysis of the COLD-SAT system and yet be applicable for use by any contractor that is elected to continue the effort. This analysis, as defined and presented in this report, should be used as the starting point for future preliminary design safety efforts.

The bulk of the work is contained in the Appendices. Appendix A contains all the hazard definitions - the detailed analysis of the potential hazards of a system given a generic situation. Appendix B contains the classification of the defined hazards, i.e. whether or not the identified hazards required preliminary design action. Both of these Appendices will be described more fully in later sections.



## II. Matrix Description

The hazard definition matrix developed for the COLD-SAT project is a three-dimensional matrix with the following matrix dimensions: Cause Category, Hazard Group, and Operational Phase. The initial matrix is shown in Figure 1. The specific items, and their definitions relative to COLD-SAT are:

### Cause Category:

- |    |                          |  |
|----|--------------------------|--|
| A. | Structural/Mechanical    | - any part of the structure or any mechanical component or system  |
| B. | Hazardous Materials      | - LH2/GH2, N2H4, components or by-products of batteries, processing solvents, etc.   |
| C. | Environmental            | - shock/vibration, temperature extremes, uninhabitable atmospheres, excessive moisture (rain or condensation), salt air, lightning, etc. |
| D. | Pneumatics/Pressurants   | - GHe, GH2, any ground operations pressurant, etc.   |
| E. | Electrical/Electronic    | - any electrical or electronic component or system   |
| F. | Ordnance                 | - pyrotechnic valves, bolt/cable cutters (no shape charges), etc.  |
| G. | Propulsion               | - N2H4, the thrusters, and the related plumbing and hardware   |
| H. | Non-Ionizing Radiation   | - generated by high-energy radio waves   |
| I. | Ground Support Equipment | - any equipment used on the program that will not be launched  |

### Hazard Group:

- |    |                        |   |
|----|------------------------|---|
| 1. | Collision/Mech. Damage | - an impact, with force, of mechanical items  |
| 2. | Corrosion              | - structural degradation of metallic or non-metallic equipment (including hydrogen embrittlement) |

**FIGURE 1 COLD-SAT HAZARD MATRIX LeRC Feasibility Study**

cause category: hazard group:	A. Structural/ Mechanical	B. Hazardous Materials	C. Environ- mental	D. Pneumatics/Electrical/ Pressurants Electronic	F. Ordnance	G. Propulsion	H. Non- Ionizing Radiation	I. Ground Support Equipment
Collision/ 1. Mechanical Damage								
2. Corrosion								
3. Contamination								
Electrical 4. Shock or Short								
5. Fire								
Explosion/ 6. Implosion								
Temperature 7. Extremes								

Operational Phases: 1. Launch site modifications 2. Subsystem manufacture 3. Transportation 4. Element Assembly  
5. Element test 6. System integration 7. System test 8. Pre-launch service  
9. Countdown 10. Flight phase I 11. Flight phase II 12. Payload separation

Hazard Group (con't):

- |    |                        |  |
|----|------------------------|--|
| 3. | Contamination          | - the release, or cause of release, of toxic, flammable, corrosive, condensible, or particulate matter |
| 4. | Electrical Shock/Short | - personnel injury or equipment damage due to improper passage of electrical current                   |
| 5. | Fire                   | - rapid oxidation of combustibles - combination of fuel, oxidizer, and an ignition source              |
| 6. | Explosion/Implosion    | - a violent release or acceptance of energy due to pressure differentials                              |
| 7. | Temperature Extremes   | - burning or freezing of skin or damage to equipment due to departure of temperature from normal       |

Operational Phase:

- |    |                           |   |
|----|---------------------------|---|
| 1. | Launch Site Modifications | - safety assessment to launch site ready          |
| 2. | Subsystem Manufacture     | - material receipt to pack and load complete      |
| 3. | Transportation            | - pack and load complete to arrival at CCAFS      |
| 4. | Element Assembly          | - arrival at CCAFS to element test start          |
| 5. | Element Test              | - element test start to system assembly start     |
| 6. | System Integration        | - system assembly start to system test start      |
| 7. | System Test               | - system test start to pre-launch servicing start |
| 8. | Pre-launch Service        | - pre-launch servicing start to countdown start   |
| 9. | Countdown                 | - countdown start to launch                       |

Operational Phase (con't):

- |                        |  |
|------------------------|--|
| 10. Flight Phase I     | - launch to arrive park orbit              |
| 11. Flight Phase II    | - arrive park orbit to arrive final orbit  |
| 12. Payload Separation | - arrive final orbit to payload separation |

The matrix was developed by taking applicable features of many different system safety hazard analysis procedures in a manner that makes it specific to COLD-SAT. Some of the references used in this development were: NSTS 22254, "Methodology for Conduct of NSTS Hazard Analyses;" S.O.I. 400-24, "Shuttle System Hazard Analysis Procedure;" and, GDSS-TC-87-006A, "Titan/Centaur Hazard Analysis Plan." The dimensions were chosen so as to be completely thorough. Therefore, there is overlap in a number of areas. The cause categories and hazard groups chosen are the items that are foreseeable as necessary for a complete evaluation on the COLD-SAT program from Feasibility Study through Launch.

### III. Hazard Definition Approach

The potential hazards were addressed by asking the generic question, "How can (cause category) cause (hazard group) during (operational phase)?" In each case a numbering system was developed to identify each matrix point according to the specific dimensions it encompassed. For example, the first hazard definition addresses the question "How can the structural/mechanical system cause collision/mechanical damage during launch site modifications?" From the matrix (Figure 2) it is seen that collision/mechanical damage is the '1' row (hazard group); structural/mechanical is the 'A' column (cause category); and, launch site modifications is the '1' operational phase. Therefore, this definition is given the title of 1.A.1.1, with the final '1' added to signify the first (of potentially others) definition.

The answer to the generic questions provided the substance of each hazard definition. The definitions were not developed until a deep understanding of the entire COLD-SAT system was obtained. In addition, prior knowledge of safety information for missile systems and satellites (or "lessons learned") was used to help obtain a baseline. The technical aspects of the definition were arrived at based on sound engineering knowledge and the acquired specific system knowledge. Each matrix point was viewed as an independent entity (i.e. the definition derived for one operational phase involving a certain cause category/hazard group did not affect the derivation of a definition for another operational phase). The definitions were then judged on their applicability to the COLD-SAT program and its various design phases. Certain hazard definitions cannot physically occur on the COLD-SAT system. These were judged to be "not applicable to COLD-SAT." All the remaining hazard definitions are applicable to COLD-SAT and will need to be responded to at some point in the design. The intent of this analysis was to determine which of these definitions need a design response as part of the feasibility study. Therefore, these definitions needed to be classified as either "not a safety concern for feasibility study" or "safety concern that should be addressed during preliminary design." The difference between these two classifications was that the second provided issues that the systems' designers would account for in the preliminary design. The first classification was used to baseline issues that will need to be addressed during future phases but are not unique enough or complex enough to require a design response during the feasibility study.

Figure 2 shows the completed hazard matrix and Appendix A1 provides all of the hazard definitions and their respective classification. The coding system used for classification is as follows:

FIGURE 2

## COLD-SAT HAZARD MATRIX LeRC Feasibility Study

20 December 1989

cause category: hazard group:	A. Structural/ Mechanical	B. Hazardous Materials	C. Environ- mental	D. Pneumatics/Electrical/ Pressurants Electronic	E.	F. Ordnance	G. Propulsion	H. Non- Ionizing Radiation	I. Ground Support Equipment
Collision/ 1. Mechanical Damage	8 9 10	N/A	e	e	e	e	8 9 12	N/A	e
2. Corrosion	e	8 9 10 11 12	8 9 10 11 12	1 9 10 11 12	e	N/A	8 9 10 11 12	N/A	e
3. Contamination	e	8 9	8 9 10 11 12	6 7 8 9 10 11	8	8	8	N/A	e
Electrical 4. Shock	N/A	N/A	9 10 11 12	N/A	6 7 8 10 11 12	8	N/A	N/A	1 8 9
5. Fire	N/A	7 8 9 10 11 12	N/A	8 9 10 11 12	8	e	8 9 10	N/A	e
6. Explosion	8	7 8 9 10 11 12	e	1 5 7 8 9 10 11 12	8 9 10 11 12	7 8 9 10 11 12	e	N/A	8 9
Temperature 7. Extremes	e	8 9 10 11 12	8 9 10 11 12	6 7 8 9 10 11 12	6 7 8 9 10 11 12	8 9 10 11 12	7 8 9 10 11 12	6 7 8	e

ORIGINAL PAGE IS  
OF POOR QUALITY

## Operational Phases:

1. Launch site modifications  
5. Element test  
9. Countdown2. Subsystem manufacture  
6. System integration  
10. Flight phase I3. Transportation  
7. System test  
11. Flight phase II4. Element Assembly  
8. Pre-launch service  
12. Payload separation

N/A - not applicable to COLD-SAT e - no definitions in this area are a safety concern

- + Not applicable to COLD-SAT
- Not a safety concern for feasibility study
- \* Safety concern that should be addressed during preliminary design

The structure of the matrix provides for 756 individual cause category/hazard group/operational phase definitions (9X7X12). Each of these matrix points, however, is not applicable to COLD-SAT. Fourteen (14) cause category/hazard group pairs were deemed to be not applicable during any operational phase. A total of forty (40) specific definitions were also deemed to be not applicable. Therefore, a total of 208 potential hazard definitions are not applicable to COLD-SAT reducing the number of potential hazard situations evaluated to 588 definitions. Of these, 408 are not a safety concern for the feasibility study leaving 140 hazard definitions that are a safety concern and should be addressed during the preliminary design. These 140 hazard definitions are indicated on the matrix with the number that corresponds to the operational phase being addressed in that definition. The cause category/hazard group pairs that are marked with "N/A" do not have any definitions since it can not be envisioned how such a situation could arise during the COLD-SAT program. The pairs marked with an "@" have definitions, but the definitions are either not a safety concern or they are not applicable to the COLD-SAT program.

#### 756 Matrix Points - Potential Hazard Definitions

208	Not Applicable for COLD-SAT (14 cause category/hazard groups + 40)
408	Not a safety concern for feasibility study
140	Safety concern that should be addressed during preliminary design
---	
756	

#### IV. Classification Approach

There are 140 hazard definitions that are classified as a "safety concern that should be addressed during preliminary design." Not all of these safety concerns have great impacts on the design, complexity, and/or cost of COLD-SAT. Therefore, a second classification system was developed in order to determine which of the identified hazards are major concerns for a feasibility study. The basic classification scheme was defined as: (1) a major safety concern for preliminary design; (2) a minor safety concern for preliminary design; or, (3) addressed during feasibility study.

The rationale for classifying these 140 hazard definitions into one of the categories was based on a number of factors. First, if an operation will be large in scope in the design effort, it was classified as a major concern. An example of this is the case of the ordnance used in this system. Although none of the proposed ordnance is believed to be of the "Category A" type (catastrophic in and of itself), the ordnance design effort is a major consideration due to the work involved in compiling the list of uses, evaluating the effects of operation on other functions, and evaluating power requirements and effects. Secondly, if an operation provides unique safety concerns, or is of catastrophic nature of itself or in its timing (i.e. during launch), it was classified as a major concern. The prime example of this is the use and handling of the liquid hydrogen. Thirdly, if an operation has safety requirements specifically mandated, it was considered to be addressed during the feasibility study. This is the case in the propulsion system design where it is required (by ESMCR 127-1 paragraph 3.11) that two barriers be present between the hydrazine and the catalyst bed until after launch. Some of the hazards were only partially addressed in this manner and therefore have been dually classified. All remaining hazards were classified as a minor safety concern. This is not to say that these hazards are not of a programmatic concern, but that normal pre-launch safety analysis and review methods will address these items at future phases and these methods will not greatly affect the design, complexity, and/or cost of the system.

#### COLD-SAT Hazards Analysis Safety Concerns Categories

* Addressed during Feasibility Study	2
- incorporated into design	
* Minor safety concern for preliminary design	106
* Partially addressed; remainder is minor safety concern	<u>19</u>
	125
* Major safety concern for preliminary design	11
* Partially addressed; remainder is major safety concern	<u>2</u>
	<u>13</u>
TOTAL COLD-SAT FEASIBILITY STUDY SAFETY CONCERNS	140



Reasons for Classification as a Major Safety Concern:

- effort involved to eliminate or control hazard (design effort and/or safety effort)
- timing of potential hazard occurrence (i.e. during countdown or launch)
- scope of potential hazard (i.e. catastrophic result)
- unique safety requirements

All items identified as a safety concern are to be tracked throughout the program's operation. This safety analysis is designed to be used at the various stages of the program as a method of thoroughly itemizing hazards and preparing for various safety reviews.

## **V. Major Safety Concerns**

A hazard was considered to be a major safety concern if it met any of the criteria presented in the preceding section. Hazards identified as a minor safety concern will be important during the various future design stages but are not considered to be "drivers" at the feasibility study phase of the program.

The following thirteen (13) definitions for a cause category/hazard group/operational phase were identified as areas that present major safety concerns:

The Structural/Mechanical system causing Collision/Mechanical damage during Countdown (1.A.9.1)

- \* Any component on the spacecraft or associated ground support equipment could cause mechanical damage if it failed prior to or during countdown. The potential hazard is that the failure goes undetected and the launch occurs. The safety engineer would rely on adequate designs, testing and quality assurance to assure that failures will not occur. Furthermore, it is critical that there are enough detection methods to alert the launch team to any failure.

The Structural/Mechanical system causing Collision/Mechanical damage during Flight Phase I (1.A.10.1)

- \* During flight phase I, the greatest amount of stress and vibration will normally occur. Any of the satellite components could fail mechanically or structurally and cause collision or mechanical damage. The system safety engineer must rely on adequate design, testing and quality assurance to assure that failures will not occur. If a failure occurs during flight phase I, there is no option for evasive or corrective actions.

Ground Support Equipment causing an Electrical Shock/Short during Launch Site Modifications (4.I.1.1)

- \* The launch site is considered ground support equipment and there will be many uses of electrical power on the launch site. System safety will evaluate the proposed launch site modifications during preliminary design to determine the potential for electrical shocks/shorts during any operation.

Pneumatics causing a Fire during Pre-launch Service (5.D.8.1)

- \* GH2 is to be loaded prior to launch. This will require all electrical service in the area to be terminated or have only spark proof electrical components in use during GH2 loading. Pad/area safety plans will address the non-mission-unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission-unique activities will be conducted via safety approved procedures.

The Structural/Mechanical system causing an Explosion during Pre-launch Service (6.A.8.1)

- \* There will be many pressure vessels used during pre-launch services that could explode/implode as a result of structural/mechanical damage. The pressures and time-lines, as well as the potential for structural/mechanical damage, need to be considered during preliminary design. Pad/area safety plans will address the non-mission-unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission-unique activities will be conducted via safety approved procedures.

Pneumatics causing an Explosion during Element Tests (6.D.5.1)

- \* There will be many element tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.

Pneumatics causing an Explosion during System Tests (6.D.7.1)

- \* There will be many system tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.

The Electrical/Electronics system causing an Explosion during Launch Site Modifications (6.E.1.1)

- \* The launch site will require explosion-proof electrical boxes on any level that may encounter LH2/GH2. This may require a major launch site modification to accommodate the handling of LH2/GH2.

Ordnance causing an Explosion during Pre-launch Service (6.F.7.1)

- \* A project list for the desired pyrotechnic applications needs to be compiled and the applications and installation sequence should be considered early in the design. System safety should be a primary contributor to this effort.

Ordnance causing an Explosion during Countdown (6.F.8.1)

- \* The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate whether the ordnance firing will impact other functions.

Ordnance causing an Explosion during Flight Phase I (6.F.9.1)

- \* The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate whether the ordnance firing will impact other functions.

Ordnance causing an Explosion during Flight Phase II (6.F.10.1)

- \* The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate whether the ordnance firing will impact other functions.

Ordnance causing an Explosion during Payload Separation (6.F.11.1)

- \* The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate whether the ordnance firing will impact other functions.

The next step was to identify the systems that each of these hazards applies to. Following the system identification, identification of safety considerations for each hazard was accomplished.

## **VI. System Design Approach to Major Safety Concerns**

By combining the information in the preceding sections a listing of the major safety concerns for each subsystem has been compiled. The following are these lists:

### STRUCTURAL SYSTEM:

\* The structural system will be designed to withstand the stress and vibration encountered during flight phase I. In addition, the design will keep spacecraft bending within the allowable payload envelope, thus avoiding contact with the faring.

\* Adequate testing will be performed to assure that spacecraft structural or mechanical failures will not occur and adequate controls will be mandated to assure conformance to the design.

### GROUND SUPPORT EQUIPMENT SYSTEM:

\* Non-mission-unique activities will follow the safety requirements of ESMCR 127-1.

\* Mission-unique activities will be conducted via safety approved procedures.

\* Pressure vessels will be designed to the requirements of MIL-STD-1522A.

\* Adequate design, testing, and quality assurance will be performed to assure that mechanical ground support equipment failures will not occur.

\* Detection methods to alert the launch team to any failure will be provided.

\* All proposed launch site modifications will be evaluated by safety to determine the potential for hazards during any operation.

\* All electrical service in the area will be terminated or have only spark-proof electrical components in use during GH2 loading; LH2 will be remotely loaded.

\* The launch site will require explosion-proof electrical boxes on any level that may encounter LH2/GH2.

### OPERATIONS:

\* Non-mission-unique activities will follow the safety requirements of ESMCR 127-1.

\* Mission-unique activities will be conducted via safety approved procedures.

- \* Mission and ground pressures and time-lines, and their hazard potential, will be evaluated by safety and submitted to range safety for analysis.

- \* The application and installation sequence of all pyrotechnic applications will be considered early in the design. Also, the sequence of ordnance activation will be evaluated to assure an adequate supply of power and to assess the impact of ordnance firing on other spacecraft functions.

#### EXPERIMENT SYSTEM:

- \* Mission-unique activities will be conducted via safety approved procedures.

- \* Mission pressures and time-lines will be compiled.

- \* Pressure vessels will be designed at a minimum to the requirements of MIL-STD-1522A.

- \* All test plans and procedures will be evaluated and approved by safety for all testing.

- \* A project list of the desired pyrotechnic applications will be compiled (including sequence of activation).

#### PROPULSION SYSTEM:

- \* Mission pressures and time-lines will be compiled.

- \* Pressure vessels will be designed to the requirements of MIL-STD-1522A.

- \* All test plans and procedures will be evaluated and approved by safety for all testing.

#### POWER SYSTEM:

- \* A project list of the desired pyrotechnic applications will be compiled (including sequence of activation).

All of the above safety considerations have become a part of the feasibility study design and the resulting baselined spacecraft. Obviously, there will be additional safety considerations as the program progresses - these should precipitate from this baseline analysis.

## **VII. Specific Safety Issues**

### Structural Design Considerations

If the structural/mechanical system caused collision or mechanical damage at any point prior to the countdown, there would be the opportunity for corrective action at a later time. At countdown, however, this opportunity does not exist. Therefore, it is imperative that any hazard of this type be detected during the countdown. The timing of this event makes it a major safety concern. Thus, the structure subsystem must have adequate design and testing to avoid any hazard, as well as adequate quality assurance programs. Secondly, the ground support equipment must provide adequate detection methods that will alert the launch team to any improper conditions.

The spacecraft and launch vehicle will encounter the greatest amount of stress and vibration during flight phase I. Therefore, this is the "worst-case" that must be designed for. The design must include accommodations for bending within the payload envelope as well as for the stress levels to be reached at this time. An adequate design and testing program and proper quality assurance provisions must be made.

### Launch Site Modifications

Due to the unique nature of COLD-SAT, extensive work will be done in the area of launch site modifications. The amount and duration of this work combine to make the launch site modifications a major safety concern. Since the bulk of this work will be accomplished at later design phases, the only safety consideration that can be itemized at this time is that all modifications desired will be done in accordance with the requirements of ESMCR 127-1. Furthermore, all modifications will be approved by range safety and the launch site contractor.

The launch site modifications will be handled by providing a COLD-SAT "mission kit" at the start of preparations for the launch. This "kit" will be comprised of the plans, procedures, and hardware necessary to accomplish all the agreed upon modifications.

### GH2, GHe, and N2H4 Loading Considerations

The loading of GH2, GHe, and N2H4 during pre-launch servicing presents a major safety concern, in addition to requiring major launch site modifications. At the time of loading, either all electrical service in the area will have to be terminated, or all components in use at this time will be required to be spark-proof. Range safety (in accordance with ESMCR 127-1) will approve all activities and will approve all plans and procedures. A significant effort is needed to design the modifications to assure

safe operations.

The ground operations plan calls for the GHe to be loaded in the Hazardous Processing Facility (HPF) using existing facilities and servicing hardware. The N2H4 will also be loaded in the HPF. The N2H4 system consists of flight qualified pressure vessels (at pressures higher than COLD-SAT is proposing) and will also use existing facilities and equipment. Access to the N2H4 is provided through the fairing should downloading of the propellant be required.

#### Pressure Vessel Design Considerations

The use of pressure vessels is a major safety concern. COLD-SAT uses pressure vessels in its experiment, its propulsion system, and in its ground support equipment. The major concern will occur during pre-launch service when the vessels are pressurized or during element and system tests. It is imperative that these vessels be designed with adequate factors of safety. Range safety has suggested designing to the requirements of MIL-STD-1522A. In addition, the pressure time-line must be evaluated and all procedures and plans must be approved by safety. Adequate safety measures will be followed, including those in ESMCR 127-1. The potential for structural or mechanical damage, and the resulting hazards, will also be evaluated.

The pressure vessel designs are in accordance with the following (although these are not necessarily requirements):

<u>Pressure Vessel</u>	<u>qty</u>	<u>specification</u>
GH2 Vaporizers	2	MIL-STD-1522A
GHe Bottles (experiment)	2	MIL-STD-1522A
N2H4 Bottles	4	MIL-STD-1522A, flight qualified
GHe Pressurant Tanks	2	MIL-STD-1522A, flight qualified
LH2 Supply Tank	1	ASME Boiler and Pressure Vessel Code, Section VIII, Division 1
LH2 Small Receiver Tank	1	ASME Boiler and Pressure Vessel Code, Section VIII, Division 1
LH2 Large Receiver Tank	1	ASME Boiler and Pressure Vessel Code, Section VIII, Division 1

#### LH2 Handling Considerations

The loading of the LH2 during pre-launch servicing presents the major safety concern, in addition to requiring major launch site modifications. Range safety (in accordance with ESMCR 127-1) will approve all activities and will approve all plans and procedures. A significant effort is needed to design the modifications to assure safe operations.

The launch site will require explosion-proof electrical boxes



and equipment on any level that may encounter LH2. This is a feature that is provided by Complex 36, due to its Centaur facilities. In order to minimize safety concerns, Centaur systems will be used as much as possible. In addition, loading will be remotely monitored and controlled from the Launch Complex Control Room.

Although the LH2 Supply Tank will be "locked-up" at T-95 sec, the capability to vent and drain will remain until the commit to launch.

### Pyrotechnic Usage/Control Considerations

Ordnance will be used in a couple of COLD-SAT applications. It will be used as part of the power system (solar array deployment) and the experiment system (GHe Purge Bag Vent). Although no projected application involves high-explosive devices (irrespective of Flight Termination System), the proper functioning of the respective pyrotechnics is essential to maintaining safety. Therefore, a list of all uses of ordnance is mandatory as is an evaluation that addresses the availability of adequate power, the sequence of activation, and the impact on other systems that the ordnance firing will have.

Due to the complexity of the COLD-SAT satellite, it was impossible to completely eliminate pyros that will not be accessible to ground personnel once the spacecraft is assembled. The occurrences were minimized to the activation of the GHe Purge Bag Vent. These pyros as well as any pyro that controls a hazardous function (i.e. LH2 flow) will be operated from a dedicated pyro control box. This box will isolate the pyros electrically until F-1 day, at which time the flight actuation cable will be installed to arm the pyros. The pyro control box will be accessible through the fairing access doors.

#### **VIIa. Flight Termination System**

The requirements of ESMCR 127-1 chapter 4 specify the use of a flight termination system (FTS) unless a waiver is granted by Range Safety. For the COLD-SAT Feasibility Study, it was assumed that an FTS was needed and the spacecraft system was designed accordingly.

The need for an FTS arises based on two concerns: (1) an intact impact of a suborbital spacecraft following premature separation from the launch vehicle; and (2) independent propulsive potential of the spacecraft. Due to the relative size of the RCS thrusters on COLD-SAT, it can be shown that the spacecraft will effectively have no independent propulsive potential. Therefore, the FTS concern is with an intact impact of the COLD-SAT LH2 and N2H4 vessels.

The FTS that was baselined for COLD-SAT is referred to as an Inadvertent Separation Destruct System (ISDS). This type of system is attached to the launch vehicle and connected to the payload by "break-wires." These "break-wires" will trigger the destruct mechanism if the payload should separate from the launch vehicle prior to the command to do so. The actual system baselined for COLD-SAT is the Martin Marietta Explosive Formed Projectile system. This system has flown on all the commercial Titans and will fly on the Titan IV/Centaur. The system is proposed to be mounted on the Centaur payload adapter thereby eliminating the concern of an inadvertent on-orbit firing.

### VIII. Conclusion/Recommendations/Issues

The conclusion reached following this feasibility study safety analysis is that there does not appear to be any safety-related reasons that would make the COLD-SAT program non-feasible. None of the major safety concerns are technical constraints. All of the safety considerations can be accomplished, albeit with some effort and cost, but do not appear to require extraordinary measures.

It is recommended that this analysis be used as the starting point for all future safety analyses. The analysis and database produced are designed to be utilized by other organizations involved with the COLD-SAT program.

However, some simple changes to the hazard matrix would be helpful in the future. First, the third dimension, operational phase, would be more accurate if described as program phase. Secondly, the program phases themselves would be more useful from a safety standpoint if they were changed as follows:

<u>FROM</u>	<u>TO</u>
10. Flight Phase I	Launch
11. Flight Phase II	Payload Separation
12. Payload Separation	On Orbit

where launch would indicate the span from lift-off to payload separation. This would allow the evaluation of on-orbit safety issues such as end-of-life operations and space debris.

The only issue or concern that arose during the analysis dealt with the lack of concrete answers available from range safety. It is understandable that they cannot provide definite answers unless a firm design exists. Therefore, suggestions (not answers) received from range safety became answers to questions and part of the design. If all future work remains within the boundaries established by the feasibility study there should not be any additional safety issues. However, if the design is significantly altered, system safety should evaluate the proposed changes for programmatic impacts. Therefore, it is imperative that all future work be done with both system safety's and range safety's knowledge, support, and approval.

## APPENDIX A1

### Hazard Definitions

## HAZARD DEFINITIONS

1. ; A.

*How can the Structural/Mechanical system cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?*

CODE	DESCRIPTION
1.A.1.1 (launch site mods.)	- No design impact for feasibility study. There are many ways that collision or mechanical damage can occur due to a mechanical/structural failure during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.
1.A.2.1 (subsystem mfg.)	- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements.
1.A.3.1 (transportation)	- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address collision or mechanical damage caused by mechanical/structural failures will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.
1.A.4.1 (element assembly)	- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be analyzed by a safety engineer and appropriate safety controls will be included in the procedures. An example of mechanical/structural failure causing collision or mechanical damage would be a failure of the supply tank test fixture mechanically failing during vibration testing because of weld defects. System safety will assure that there adequate quality controls to produce conforming welds.
1.A.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for mechanical/structural failure that could cause collision or mechanical damage during the element tests, the system engineer will assure that appropriate safety measures are known and in place.

- 1.A.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all tests for potential safety impacts. Upon determination that a process has potential for mechanical/structural failure that could cause collision or mechanical damage during system integration, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.A.7.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for mechanical/structural failure that could cause collision or mechanical damage during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.A.8.1 (prelaunch services) \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures (example of non-mission unique safety consideration: Personnel platforms structurally fail causing injury to personnel of damage to the satellite; example of a mission unique safety consideration: The LH2 supply line support brackets fracture resulting in damage to the line).
- 1.A.9.1 (countdown) \* This could be a design impact that should be considered during preliminary design. Any component on the spacecraft or associated GSE could cause damage if it failed during countdown. The safety engineer would rely on adequate designs, testing and QA to assure that failures will not occur. The potential hazards are that the failure goes undetected and the launch occurs. Therefore, it is critical that there are enough detection methods to alert the launch team to these failures.
- 1.A.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. During flight phase I, the greatest amount of stress and vibration will normally occur. Any of the satellite components could fail mechanically or structurally and cause collision or mechanical damage. In addition, the nose faring or its components could fail and impact the satellite. The system safety engineer must rely on adequate design, testing and QA to assure that failures will not occur. If a failure occurs during flight phase I, there is no option for evasive or corrective actions.

1.A.11.1.1 (flight phase II)

- No design impact for feasibility study. Any of the satellite components could fail mechanically or structurally and cause mechanical damage. The system safety engineer must rely on adequate design, testing and QA to assure that failures will not occur. If a failure occurs during flight phase II, there is no option for evasive or corrective actions.

1.A.12.1 (payload separation)

- No design impact for feasibility study. A mechanical/structural failure of the separation system could cause collision or mechanical damage to the satellite. Also, re-contact of the launch vehicle after separation could cause damage. The separation system is a critical single point failure; the system safety engineer should review the separation system and sequence to assure that there is adequate verification that it will perform its intended functions.

Author's notes: How can the Structural/Mechanical system cause Collision/Mechanical Damage during \_\_\_\_\_  
Operational Phase?

## HAZARD DEFINITIONS

1. ; B.

How can Hazardous Materials cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how hazardous materials could cause collision/mechanical damage during any of the operational phases.

Hazardous Materials, by themselves, cannot cause collision or mechanical damage. Any collision or mechanical damage would result from a second order failure. The initial failure modes will be addressed elsewhere in this hazards analysis.

26

Author's notes: How can Hazardous Materials cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

Hazardous materials that will be associated with COLD-SAT, such as LH2/GH2, N2H4, components or by-products of batteries, or solvents used in processing, by themselves will not cause collision or mechanical damage. If these materials caused an explosion or a violent reaction, the high energy fragments could cause a collision or mechanical damage. These hazards are addressed in 6.B, Hazardous Materials causes Explosion.



## HAZARD DEFINITIONS

1. ; C.

How can Environmental conditions cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Environmental conditions could cause Collision/Mechanical damage during any of the operational phases.

Author's notes: How can Environmental conditions cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

Environmental conditions are: shock/vibration; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; etc. The results of these environmental conditions can create the potential for hazards. At the feasibility study phase of this program, methods for environmental conditions causing collision/mechanical damage are indeterminable.

## HAZARD DEFINITIONS

1. ; D.

How can Pneumatics cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
1.D.1.1.1 (launch site mods.)	- No design impact for feasibility study. From the current information it can not be determined how pneumatics could cause collision or mechanical damage during launch site modifications.
1.D.2.1 (subsystem mfg.)	- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
1.D.3.1 (transportation)	- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address pneumatics causing collision or mechanical damage will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.
1.D.4.1 (element assembly)	- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When pneumatics are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent collision or mechanical damage. The potential for hazards will be reported to NASA via safety plans.
1.D.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for collision or mechanical damage caused by pneumatics during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
1.D.6.1 (system integration)	- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for collision or mechanical damage caused by pneumatics, the safety engineer will assure that appropriate safety measures are known and in place.

1.D.7.1 (system test)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a system test has potential for collision or mechanical damage caused by pneumatics, the safety engineer will assure that appropriate safety measures are known and in place.

1.D.8.1 (prelaunch services)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Pneumatic vents that will be used during prelaunch servicing will need to be located and directed away from structures that could be damaged from the venting pressure.

1.D.9.1 (countdown)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Pneumatic vents that will be used during countdown will need to be located and directed away from structures that could be damaged from the venting pressure.

1.D.10.1 (flight phase I)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Pneumatic vents that will be used during flight will need to be located and directed away from structures that could be damaged from the venting pressure.

2 1.D.11.1 (flight phase II)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Pneumatic vents that will be used during flight will need to be located and directed away from structures that could be damaged from the venting pressure.

1.D.12.1 (payload separation)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Pneumatic vents that will be used during payload separation will need to be located and directed away from structures that could be damaged from the venting pressure.

Author's notes: How can Pneumatics cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

Pneumatics or Pressurant escaping gas could impact and damage items directly and cause collision or mechanical damage or it could cause items to be projectiles, which could cause them to collide and cause mechanical damage.

Pneumatics or pressurants by themselves can not cause collision or mechanical damage. An over-pressure condition could result in mechanical damage. This condition is addressed in 6.D, Pneumatics causes Explosion/Implosion. Collision or mechanical damage could cause a pneumatic or pressurant leak and the escaping gas could be a hazard. If the escaping gas caused Temperature Extremes, a Fire, Contamination or Corrosion the potential hazards are addressed in those respective Hazard Groups. This hazard analysis will only address planned release of pneumatics or pressurants. An unplanned release of pressure is the result of a failure and therefore is a second order failure. The potential for initial failures are addressed in other sections of this hazard analysis.

## HAZARD DEFINITIONS

1. ; E.

How can the Electrical/Electronics system cause Collision/Mechanical damage during \_\_\_\_ Operational Phase?

CODE

DESCRIPTION

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Electrical/Electronics failures could cause Collision/Mechanical damage during any of the operational phases.

Author's notes: How can the Electrical/Electronics system cause Collision/Mechanical damage during \_\_\_\_ Operational Phase?

ω An Electrical/Electronics failure could cause Collision/Mechanical damage by causing an unexpected  
O activation/operation of equipment. This is a second order failure and will be addressed elsewhere in the hazard analysis as a first order effect.

## HAZARD DEFINITIONS

1. ; F.

How can Ordnance cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
1.F.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Ordnance is not typically included as part of launch site modifications. If ordnance are part of launch site modification, the site safety officer should be knowledgeable of their presence and take appropriate actions. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
1.F.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li></ul>
1.F.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials (including ordnance). The "program hazardous materials list" will be used to identify the hazards that are associated with each material and their effects.</li></ul>
1.F.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When ordnance is to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent collision or mechanical damage from the ordnance. The potential for hazards will be reported to NASA via safety plans.</li></ul>
1.F.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test may use ordnance that could cause collision or mechanical damage during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</li></ul>

- 1.F.6.1 (system integration)
- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for collision or mechanical damage resulting from ordnance, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.F.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for collision or mechanical damage caused by ordnance, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.F.8.1 (prelaunch services)
- No design impact during feasibility study. The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments that could cause collision or mechanical damage. Ordnance are usually installed during prelaunch services either at the hazardous processing facility or at the launch pad. A band clamp type separation system is currently being proposed for COLD-SAT. This system has frangible bolts that are self contained and will not produce high energy fragments that could cause collision or mechanical damage. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 1.F.9.1 (countdown)
- No design impact during feasibility study. The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments that could cause collision or mechanical damage. The use of ordnance will be monitored by the system safety engineer to determine if ordnance that could cause collision or mechanical damage is proposed for the program.
- 1.F.10.1 (flight phase I)
- No design impact during feasibility study. The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments that could cause collision or mechanical damage. The use of ordnance will be monitored by the system safety engineer to determine if ordnance that could cause collision or mechanical damage is proposed for the program.
- 1.F.11.1 (flight phase II)
- No design impact during feasibility study. The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments that could cause collision or mechanical damage. The use of ordnance will be monitored by the system safety engineer to determine if ordnance that could cause collision or mechanical damage is proposed for the program.

1.F.12.1 (payload separation) - No design impact during feasibility study. The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments that could cause collision or mechanical damage. The use of ordnance will be monitored by the system safety engineer to determine if ordnance that could cause collision or mechanical damage is proposed for the program.

Authors notes: How can Ordnance cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

Ordnance can cause collision or mechanical damage if they produce high energy fragments upon activation. A system such as a shape charge that has an external explosion has the potential to produce a collision or mechanical damage. Most ordnances, such as cable and bolt cutters, are contained and do not have the potential for producing high energy fragments.

## HAZARD DEFINITIONS

1. ; G.

How can Propulsion cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
1.G.1.1 (launch site mods.)	+ Not applicable: this phase does not apply to the cause category/hazard group. There is no propulsive elements involved in this phase of the program.
1.G.2.1 (subsystem mfg.)	+ Not applicable: this phase does not apply to the cause category/hazard group. There is no propulsive elements involved in this phase of the program.
1.G.3.1 (transportation)	+ Not applicable: this phase does not apply to the cause category/hazard group. There is no propulsive elements involved in this phase of the program.
1.G.4.1 (element assembly)	+Not applicable: this phase does not apply to the cause category/hazard group. There is no propulsive elements involved in this phase of the program.
1.G.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for element testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for propulsion causing collision/mechanical damage during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
1.G.6.1 (system integration)	+ Not applicable: this phase does not apply to the cause category/hazard group. There is no propulsive elements involved in this phase of the program.
1.G.7.1 (system test)	- No design impact during feasibility study. Test plans/procedures will be required for system testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for propulsion causing collision/mechanical damage during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
1.G.8.1 (prelaunch services)	* This could be a design impact that should be considered during the preliminary design. To satisfy the requirements of ESMCR 127-1, there must be two barriers between the N2H4 and the catalyst beds. These barriers (valves) must be included in the design.



1.G.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. To satisfy the requirements of ESMCR 127-1, there must be two barriers between the N2H4 and the catalyst beds until after lift off. These barriers (valves) must be included in the design.

1.G.10.1 (flight phase I)

+ Not applicable: this phase does not apply to the cause category/hazard group. If a thruster were to activate during flight phase I, the contamination would have a greater impact than any collision/mechanical damage. That is addressed in hazard category 3.G, Propulsion causing Contamination.

1.G.11.1 (flight phase II)

+ Not applicable: this phase does not apply to the cause category/hazard group. If a thruster were to activate during flight phase II, the contamination would have a greater impact than any collision/mechanical damage. That is addressed in hazard category 3.G, Propulsion causing Contamination.

1.G.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Re-contact after separation could occur if an RCS thruster fires upon or after separation. The RCS system needs to be designed to withstand the shock of separation without allowing N2H4 to leak onto the catalyst bed.

Author's notes: How can Propulsion cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

The inadvertent firing of an RCS thruster(s) could cause collision/mechanical damage. In order for a thruster to fire, hydrazine must be present on the catalyst bed. Hydrazine may be present during testing or after N2H4 loading, during prelaunch services. The on-board system will have isolation valves to prevent N2H4 from entering the thruster loop until after t-0. Redundant thruster valving will prevent the N2H4 from entering the REMs until the valves are commanded open.

## HAZARD DEFINITIONS

1. ; H.

How can Non-Ionizing Radiation cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Non-Ionizing Radiation can not cause Collision/Mechanical damage on the satellite or the launch site. The ground stations, where non-ionizing radiation would be a concern, is not included in this analysis.

Author's notes: How can Non-Ionizing Radiation cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves. The level of non-ionizing radiation from the spacecraft antenna is very low and is very unlikely to cause injury to personnel. The communication GSE where high energy radio waves are used is not included in this analysis.

## HAZARD DEFINITIONS

1. ; l.

How can Ground Support Equipment cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
1.I.1.1 (launch site mods.)	<p>- No design impact for feasibility study. There are many ways that GSE could cause collision/mechanical damage during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</p>
1.I.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements. Good engineering design practices and testing will be relied upon to assure adequate margins of safety on GSE. The manufacturing of GSE will be performed per the specifications of the drawings and contracts. Quality Assurance will be relied upon to assure conformance to the specifications.</p>
1.I.3.1 (transportation)	<p>- No design impact for feasibility study. GSE will be used extensively during transportation for the satellite and its associated equipment. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address collision/mechanical damage caused by GSE will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority. Good engineering design practices and testing will be relied upon to assure adequate margins of safety on GSE. The manufacturing of GSE will be performed per the specifications of the drawings and contracts. Quality Assurance will be relied upon to assure conformance to the specifications.</p>
1.I.4.1 (element assembly)	<p>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When GSE is to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the collision/mechanical damage. The potential for hazards will be reported to NASA via safety plans. Good engineering design practices and testing will be relied upon to assure adequate margins of safety on GSE. The manufacturing and assembly of GSE will be performed per the specifications of the drawings and contracts. Quality Assurance will be relied upon to assure conformance to the specifications.</p>

- 1.I.5.1 (element test)
  - No design impact during feasibility study. The testing of GSE and the use of GSE in element tests needs to be considered for its potential impacts on system safety. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that GSE may cause a hazard during element testing, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.I.6.1 (system integration)
  - No design impact during feasibility study. GSE will be used during system integration and its failures could cause collision/mechanical damage in many ways. Good engineering design practices and testing will be relied upon to assure adequate margins of safety on GSE. The manufacturing and assembly of GSE will be performed per the specifications of the drawings and contracts. Quality Assurance will be relied upon to assure conformance to the specifications. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for GSE to cause collision/mechanical damage, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.I.7.1 (system test)
  - No design impact during feasibility study. GSE will be system tested and will be used during system testing. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for GSE to cause collision/mechanical damage during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 1.I.8.1 (prelaunch services)
  - No design impact during feasibility study. GSE will be used extensively during prelaunch services. Plans/procedures will be required for all operations performed during prelaunch servicing. System safety will consider all operations for potential safety impacts. Upon determination that an operation has potential for GSE to cause collision/mechanical damage, the safety engineer will assure that appropriate safety measures are known and in place. The pad/area safety requirements, such as those in ESMCR 127-1, chapter 5, will be used to control many of the prelaunch servicing operations.
- 1.I.9.1 (countdown)
  - No design impact during feasibility study. There are many ways that GSE could fail and cause collision/mechanical damage during countdown. Good engineering design practices and testing will be relied upon to assure adequate margins of safety on GSE. The manufacturing of GSE will be performed per the specifications of the drawings and contracts. Quality Assurance will be relied upon to assure conformance to the specifications. There will be adequate detection and sensing devices on the GSE and space bound systems to determine if collision/mechanical damage has occurred during countdown.
- 1.I.10.1 (flight phase I)
  - + Not applicable: this phase does not apply to the cause category/hazard group.

1.I.11.1 (flight phase II) + Not applicable: this phase does not apply to the cause category/hazard group.

1.I.12.1 (payload separation) + Not applicable: this phase does not apply to the cause category/hazard group.

Author's notes: How can Ground Support Equipment cause Collision/Mechanical damage during \_\_\_\_\_ Operational Phase?

There are many ways that GSE could cause collision/mechanical damage during all phases of the program where GSE is used. Examples are a step stool could fall from the launch vehicle service tower and damage the vehicle or a pressure line on a test service cart could rupture and the shrapnel could damage the spacecraft components or a transport dolly could fracture and damage the satellite.

The design of GSE usually follows the satellite design and therefore would not normally be a subject for the preliminary design. The possible exception to that is if existing equipment is to be used or modified for use on COLD-SAT. System safety should evaluate any GSE that is proposed for use for its potential hazards.

## HAZARD DEFINITIONS

2 ; A.

How can the Structural/Mechanical system cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.A.1.1 (launch site mods.)	<p>- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. This is a time-related event and will be considered in the design, manufacturing, and construction of equipment. System safety will rely on the designers and manufacturers to assure that consideration is given to corrosion and its potential as a safety hazard. Site safety checks will be conducted periodically in an attempt to identify safety hazards related to structural/mechanical conditions that could cause corrosion.</p>
2.A.2.1 (subsystem mfg.)	<p>- No design impact during feasibility study. Structural/mechanical conditions that could cause corrosion will be considered during the design and manufacturing of subsystems. The potential as safety hazards will be considered by the designer and by the project safety engineer.</p>
2.A.3.1 (transportation)	<p>- No design impact during feasibility study. The environmental conditions during transportation will be considered during the design of the hardware. The potential as safety hazards will be considered by the designer and by the project safety engineer. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address the potential for corrosion caused by structural/mechanical damage will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.</p>
2.A.4.1 (element assembly)	<p>- No design impact during feasibility study. Structural/mechanical conditions that could cause corrosion will be considered during the element assemblies. The potential as safety hazards will be considered by the designer and by the project safety engineer.</p>
2.A.5.1 (element test)	<p>- No design impact during feasibility study. The environmental conditions during element testing will be considered during the design of the hardware and during test development. The potential for safety hazards will be considered by the test engineer and by the project safety engineer.</p>

- 2.A.6.1 (system integration) - No design impact during feasibility study. Structural/mechanical conditions that could cause corrosion will be considered during system integration. The potential as safety hazards will be considered by the designer and by the project safety engineer.
- 2.A.7.1 (system test) - No design impact during feasibility study. The environmental conditions during system testing will be considered during the design of the hardware and during test development. The potential for safety hazards will be considered by the test engineer and by the project safety engineer.
- 2.A.8.1 (prelaunch services) - No design impact during feasibility study. Currently, it can not be conceived how the electrical/electronics system could cause corrosion during prelaunch services. Corrosion is a time-related function.
- 2.A.9.1 (countdown) - No design impact during feasibility study. Currently, it can not be conceived how the electrical/electronics system could cause corrosion during countdown. Corrosion is a time-related function and the countdown is a short duration event.
- 2.A.10.1 (flight phase I) - No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during flight. Corrosion is a time-related function and the flight phase is a short duration event.
- 2.A.11.1 (flight phase II) - No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during flight. Corrosion is a time-related function and the flight phase is a short duration event.
- 2.A.12.1 (payload separation) - No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during payload separation. Corrosion is a time-related function and the payload separation is a short duration event.

Author's notes: How can the Structural/Mechanical system cause Corrosion during \_\_\_\_\_ Operational Phase?

When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as the pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has catastrophic result.

Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards. The project approved materials and processing list will identify materials that can be used in gaseous and liquid hydrogen environments. System safety will verify that only approved materials will be specified for use in specific applications.

## HAZARD DEFINITIONS

2. ; B.

How can Hazardous Materials cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.B.1.1 (launch site mods.)	<p>- No design impact for feasibility study. The design lacks sufficient details to evaluate for potential safety hazards. There are many ways that hazardous materials can cause corrosion at the launch site during modifications. The standard facility safety requirements and existing systems will be relied upon to control hazards during site modifications, including the requirements of ESMCR 127-1, chapter 5.</p>
2.B.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements. The program materials lists will identify all hazardous materials and include a description of the hazards associated with each material.</p>
2.B.3.1 (transportation)	<p>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards, and their corrosive effects, that are associated with each material.</p>
2.B.4.1 (element assembly)	<p>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When hazardous materials are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the corrosive effects. The potential for hazards will be reported to NASA via safety plans.</p>
2.B.5.1 (element test)	<p>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for the use of hazardous materials that could cause corrosion. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. Upon determination that a test has potential for corrosion from hazardous materials during the element tests, the safety authority will assure that appropriate safety measures are known and in place.</p>



- 2.B.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all tests for potential safety impacts. Upon determination that an integration process includes hazardous materials that could cause corrosion, the safety authority will assure that appropriate safety measures are known and in place.
- 2.B.7.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for the use of hazardous materials that could cause corrosion. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. Upon determination that a system test has potential for corrosion from hazardous materials, the safety authority will assure that appropriate safety measures are known and in place.
- 2.B.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during prelaunch services. Design methods will be identified to reduce the impact of these hazards.
- 2.B.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during countdown. Design methods will be identified to reduce the impact of these hazards. Normally, corrosion is a time-related (slow) process which would not occur during the ground processing through payload separation phases.
- 2.B.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during launch phase I. Design methods will be identified to reduce the impact of these hazards. Normally, corrosion is a time-related (slow) process which would not occur during the ground processing through satellite end of life.
- 2.B.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during launch phase II. Design methods will be identified to reduce the impact of these hazards. Normally, corrosion is a time-related (slow) process which would not occur during the ground processing through satellite end of life.

2.B.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during payload separation. Design methods will be identified to reduce the impact of these hazards. Normally, corrosion is a time-related (slow) process which would not occur during the ground processing through satellite end of life.

Author's notes: How can Hazardous Materials cause Corrosion during \_\_\_\_\_ Operational Phase?

Hazardous materials need to be controlled. They can be in a solid, liquid or gaseous state or a combination of these states. A project approved materials list will be compiled. It will include the hazards or hazardous conditions for each material that will be used on the project. Methods for controlling these hazardous materials will be considered during the preliminary design phase of the program. Corrosion caused by the hazardous materials (such as the electrolyte in the batteries) will be addressed as the materials are identified.

Corrosion could occur during use in space, provided the proper elements and conditions are present. Corrosion during on orbit time is a mission success issue but is not a system safety concern.

## HAZARD DEFINITIONS

2 ; C.

How can Environmental conditions cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.C.1.1 (launch site mods.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There are many ways that environmental conditions could cause corrosion at the launch site such as the salt air environment at CCAFS. The launch complexes have active maintenance programs that are intended to identify areas of corrosion and correct any potential hazards. Site safety personnel will be active participants in the design and drawing reviews of launch site modification. They will be relied upon to identify any potential hazards and conformance to the safety requirements, such as ESMCR 127-1.</p>
2.C.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There will be many opportunities for environmental conditions to introduce the elements of corrosion during subsystem manufacturing. The subsystem manufacturers will be required to adhere to the requirements of the "program approved materials list". The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</p>
2.C.3.1 (transportation)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There will be many opportunities for environmental conditions to introduce the elements of corrosion during transportation. Handling and transportation plans will be required for all subassemblies and assemblies. The expected environmental conditions and methods to prevent contamination that could cause corrosion will be included in these plans. These transportation plans will be reviewed and approved by a project safety authority.</p>
2.C.4.1 (element assembly)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There will be many opportunities for environmental conditions to introduce the elements of corrosion during element assembly. Element assembly will be performed via approved assembly procedures. System safety will be an active participant in the review and approval of the assembly procedures. The potential for environmental conditions causing corrosion will be considered during this review.</p>

- 2.C.5.1 (element test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that could introduce the elements of corrosion during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.C.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for environmental conditions introducing an element of corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.C.7.1 (system test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that could introduce an element of corrosion during the tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.C.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Many systems will be opened and exposed to the environment that could introduce elements of corrosion during prelaunch servicing. These operations need to be performed by experienced personnel and require adherence to approved procedures. The equipment designs need to include safeguards to prevent the introduction of contaminants during prelaunch services. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.
- 2.C.9.1 (countdown)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Environments such as purge gas could introduce elements of corrosion during countdown. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.
- 2.C.10.1 (flight phase I)
- No design impact during feasibility study. It currently can not be conceived how environmental conditions could introduce elements of corrosion during the flight phase.
- 2.C.11.1 (flight phase II)
- No design impact during feasibility study. It currently can not be conceived how environmental conditions could introduce elements of corrosion during the flight phase.

2.C.12.1 (payload separation) - No design impact during feasibility study. It currently can not be conceived how environmental conditions could introduce elements of corrosion during the payload separation.

Author's notes: How can Environmental conditions cause Corrosion during \_\_\_\_\_ Operational Phase?

Environmental conditions are: shock/vibration; G-loading; zero-G; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; etc. The results of these environmental conditions can create the potential for corrosion that could result in a catastrophic failure.

Oxidation (a type of corrosion) occurs when a ferrous material comes in contact with a salt based solution. When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as the pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result.

Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards. The project approved materials and processing list will identify materials that can be used in gaseous and liquid hydrogen environments. System safety will verify that only approved materials will be specified for use in specific applications.

A "project approved materials list" will be compiled for the COLD-SAT project. Exposure to environmental conditions that could cause corrosion will be considered as part of the evaluation for approval. System safety will be an active participant in the review and approval of materials for the approved materials list.

## HAZARD DEFINITIONS

2 ; D.

How can Pneumatics cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.D.1.1 (launch site mods.)	<p>* This could be a design impact that should be considered during the preliminary design. A hydrogen supply and loading system will be added to the launch site and hydrogen embrittlement is a potential problem during or after launch site modifications. The primary means of controlling hydrogen embrittlement is to use materials that are approved for use in hydrogen environments. The project approved materials list will be used to control material selections. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</p>
2.D.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. The project approved materials and processing list will be used to convey the concerns and inform the subsystem manufacturers of the potential hazards. Processes that include pneumatics that could cause corrosion will be included in the project approved processing list. The approved processing list will be initiated during the preliminary design. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</p>
2.D.3.1 (transportation)	<p>+ Not applicable: this phase does not apply to the cause category/hazard group.</p>
2.D.4.1 (element assembly)	<p>- No design impact for feasibility study. The project approved materials and processing list will be used to convey the concerns and inform the element assemblers of the potential hazards. Processes that include pneumatics that could cause corrosion will be included in the project approved processing list. The approved processing list will be initiated during the preliminary design. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures.</p>
2.D.5.1 (element test)	<p>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics that could cause corrosion damage during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</p>

- 2.D.6.1 (system integration)
- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for pneumatics that could cause corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.D.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics that could cause corrosion during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.D.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement will be considered during the preliminary design and proper materials can be considered for those areas of concern. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 2.D.9.1 (countdown)
- \* This could be a design impact and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.
- 2.D.10.1 (flight phase I)
- \* This could be a design impact and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.
- 2.D.11.1 (flight phase II)
- \* This could be a design impact and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.

2.D.12.1 (payload separation) \* This could be a design impact and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.

Author's notes: How can Pneumatics cause Corrosion during \_\_\_\_\_ Operational Phase?

For the COLD-SAT project, hydrogen embrittlement will be considered corrosion. GH2 will be used as a pressurant and can cause hydrogen embrittlement in some metals. The project approved materials and processing list will identify materials that can be used in a gaseous hydrogen environment. System safety will verify that only approved materials will be specified for use in specific applications.



## HAZARD DEFINITIONS

2 ; E.

How can the Electrical/Electronics system cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.E.1.1 (launch site mods.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion. The launch site modification that will be required for COLD-SAT will include the LH2 loading system. There will be electrical/electronics controls included in that system and the potential for corrosion will exist.</p>
2.E.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion during subsystem manufacturing. The potential for corrosion could be introduced during the subsystem manufacturing. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</p>
2.E.3.1 (transportation)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion during transportation. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. These transportation plans will be reviewed and approved by a project safety authority.</p>
2.E.4.1 (element assembly)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion during element assembly. The potential for corrosion could be introduced during the element assemblies. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. The potential for hazards will be reported to NASA via safety plans.</p>

- 2.E.5.1 (element test)
- No design impact during feasibility study. The tests are not specified in sufficient detail to evaluate for their safety impacts at the feasibility study. When the test plans are written, system safety will consider them for potential safety impacts. Upon determination that a test has potential for corrosion caused by electrical/electronics, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.E.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion during system integration. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for the components of corrosion being introduced during system integration, the system safety engineer will assure that appropriate safety measures are known and in place.
- 2.E.7.1 (system test)
- No design impact during feasibility study. The tests are not specified in sufficient detail to evaluate for their safety impacts at the feasibility study. Test plans/procedures will be required for all testing. When the test plans are written, system safety will review and consider them for potential safety impacts. Upon determination that a test has potential for corrosion caused by electrical/electronics, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.E.8.1 (prelaunch services)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to evaluate the potential for electrical/electronics causing corrosion during prelaunch services. There will be many prelaunch services that will provide the potential for corrosion caused by electrical/electronics. The services will be performed via plans and procedures. The system safety authority will review all plans to determine if there is a potential for electrical/electronics causing corrosion. Upon determination that a test has potential for corrosion caused by electrical/electronics, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.E.9.1 (countdown)
- No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during countdown. Corrosion is a time-related function and the countdown is a short duration event.
- 2.E.10.1 (flight phase I)
- No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during flight. Corrosion is a time-related function and the flight phase is a short duration event.
- 2.E.11.1 (flight phase II)
- No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during flight. Corrosion is a time-related function and the flight phase is a short duration event.

2.E.12.1 (payload separation) - No design impact during feasibility study. Currently, it can not be conceived how electrical/electronics could cause corrosion during payload separation. Corrosion is a time-related function and payload separation is a short duration event.

Author's notes: How can the Electrical/Electronics system cause Corrosion during \_\_\_\_\_ Operational Phase?

Electrical current is the movement of electrons along a conductive path. Electrons passing through dissimilar metals will contribute to corrosion. Chassis grounds can create this condition. The use of chassis grounds is not acceptable practice for space flight equipment or its associated ground support equipment.

Oxidation (a type of corrosion) occurs when a ferrous material comes in contact with a salt based solution. When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as the pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result.

Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards. The project approved materials and processing list will identify materials that can be used in gaseous and liquid hydrogen environments. System safety will verify that only approved materials will be specified for use in specific applications.

**HAZARD DEFINITIONS**

2. ; F.

How can Ordnance cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how ordnance can cause corrosion during any of the operational phases.

Author's notes: How can Ordnance cause Corrosion during \_\_\_\_\_ Operational Phase?

Oxidation (a type of corrosion) occurs when a ferrous material comes in contact with a salt based solution. When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as the pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result.

Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards. The project approved materials and processing list will identify materials that can be used in gaseous and liquid hydrogen environments. System safety will verify that only approved materials will be specified for use in specific applications.

## HAZARD DEFINITIONS

2. ; G.

How can Propulsion cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.G.1.1 (launch site mods.)	<p>+ Not applicable: this phase does not apply to the cause category/hazard group. The launch site is not included in the RCS. The scope of the 2.G evaluation will be limited to the COLD-SAT satellite propulsion system. The propulsion system includes the N2H4 pressurization subsystem, the N2H4 bottles, lines, valves and reaction control modules.</p>
2.G.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</p>
5 2.G.3.1 (transportation)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. The transportation plans will be reviewed and approved by a project safety authority.</p>
2.G.4.1 (element assembly)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When there is the potential for the propulsion system to introduce corrosive elements, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the corrosive effects. The potential for hazards will be reported to NASA via safety plans.</p>
2.G.5.1 (element test)	<p>- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts including the introduction of corrosive elements from or into the propulsion system. Upon determination that a test has potential for propulsion causing corrosion during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</p>

- 2.G.6.1 (system integration) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for propulsion to cause corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.G.7.1 (system test) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for propulsion causing corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.G.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. The current design includes two barriers between the N2H4 supply and the catalyst beds of the REMs which will be in effect during prelaunch servicing. The servicing equipment designs will need to be analyzed for its adherence to the pad/area safety requirements, such as those stated in ESMCR 127-1, chapter 5. The mission unique activities will be conducted via safety approved procedures.
- 2.G.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The current design includes two barriers between the N2H4 supply and the catalyst beds of the REMs which will be in effect during countdown. The operation performed during countdown concerning the propulsion system will need to be analyzed for the potential for propulsion to cause corrosion and for adherence to safety requirements, such as those stated in ESMCR 127-1, chapter 5.
- 2.G.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. The flight sequence needs to be evaluated for potential safety hazards.
- 2.G.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. The flight sequence needs to be evaluated for potential safety hazards.

2.G.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. With the N2H4 in the lines during payload separation there is the potential for a fault that would fire the REMs and initiate or cause corrosion. The flight sequence needs to be evaluated for potential safety hazards.

Author's notes: How can Propulsion cause Corrosion during \_\_\_\_\_ Operational Phase?

The scope of the 2.G evaluation will be limited to the COLD-SAT satellite propulsion system. The propulsion system includes the N2H4 pressurization subsystem, the N2H4 bottles, lines, valves and reaction control modules.

N2H4 causing corrosion is addressed in 2.B, "Hazardous Materials cause Corrosion".

The products or results of "propulsion" may include: thrust, heat, combustion and/or by-products of combustion.

The heat, combustion or by-products of combustion could contribute to corrosion. Also, hydrazine is a corrosive liquid and reacts with some metals and reacts violently with some oxides.

Oxidation (a type of corrosion) occurs when a ferrous material comes in contact with a salt based solution. When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as the pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result. System safety will verify that only approved materials will be specified for use in specific applications.

## HAZARD DEFINITIONS

2 ; H.

How can Non-Ionizing Radiation cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how non-ionizing radiation can cause corrosion during any of the operational phases.

Author's notes: How can Non-Ionizing Radiation cause Corrosion during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves.

The communication GSE where high energy radio waves are used is not included in this analysis.

When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as a pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result. Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards.



## HAZARD DEFINITIONS

2. ; I.

How can Ground Support Equipment cause Corrosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
2.I.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There are many ways that GSE can cause corrosion during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li> </ul>
2.I.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li> </ul>
2.I.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for GSE will be stated in the requirements documentation. System safety will review the transportation plans and evaluate the potential safety hazards associated with GSE causing corrosion.</li> </ul>
2.I.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. Assembly procedures will be written and used for major GSE. The assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. This includes the potential for GSE to cause corrosion. The potential for hazards will be reported to NASA via safety plans.</li> </ul>
2.I.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Test plans/procedures will be required for the product verification testing. System safety will consider these tests for potential safety impacts. Upon determination that a test has potential for GSE causing corrosion, the safety engineer will assure that appropriate safety measures are known and in place.</li> </ul>

59

- 2.I.6.1 (system integration) - No design impact during feasibility study. GSE system integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that GSE has the potential for causing corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.I.7.1 (system test) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all major GSE testing. System safety will consider these tests for potential safety impacts. Upon determination that a test has potential for GSE to cause corrosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 2.I.8.1 (prelaunch services) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used during prelaunch servicing. An operation instruction will be used for each operation. The area system safety authority will review these procedures for potential safety hazards, including methods for GSE to cause corrosion.
- 2.I.9.1 (countdown) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used during launch to monitor the spacecraft.
- 2.I.10.1 (flight phase I) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used during launch to monitor the spacecraft.
- 2.I.11.1 (flight phase II) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used during launch to monitor the spacecraft.

2.I.12.1 (payload separation) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used during launch to monitor the spacecraft.

Author's notes: How can Ground Support Equipment cause Corrosion during \_\_\_\_\_ Operational Phase?

If GSE can provide one element required for corrosion, then it can be a cause of corrosion. The elements are ferrous materials, two or more unprotected metals of different electrical potentials in contact, an electrolytic solution or electrical potential.

Oxidation (a type of corrosion) occurs when a ferrous material comes in contact with a salt based solution. When two metals of different potential are in contact and an electrolyte solution (such as salt air) is present, corrosion will occur. This process is time-related and dependent on the potential difference of the materials and the strength and quantity of the electrolyte solution. When the materials are stressed such as a pre-load of bolts, rivets or welds the corrosion is accelerated. An insulator between the materials or the absence of the electrolyte will prevent corrosion that could cause mechanical damage. There is a potential for a safety hazard when corrosion results in a failure that has a catastrophic result.

Hydrogen embrittlement is considered a type of corrosion and should be evaluated for its potential for safety hazards. The project approved materials and processing list will identify materials that can be used in gaseous and liquid hydrogen environments. System safety will verify that only approved materials will be specified for use in specific applications.

## **HAZARD DEFINITIONS**

3. ; A.

How can the Structural/Mechanical system cause Contamination during \_\_\_\_\_ Operational Phase?

<b>CODE</b>	<b>DESCRIPTION</b>
3.A.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There are many ways that contamination can occur due to structural/mechanical conditions during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5. LOX cleaning and verification procedures will be required for all LOX/GOX systems and related support equipment.</li></ul>
3.A.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The subsystem manufacturers will be required to have a contamination control program that is commensurate with the cleanliness requirements for their subsystems. Potential safety hazards will be identified by the system engineer and the safety engineer. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li></ul>
3.A.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address contamination caused by the structural/mechanical system will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.</li></ul>
3.A.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The element assembly operations will be required to have a contamination control program that is commensurate with the cleanliness requirements for their subsystems. Potential safety hazards will be identified by the system engineer and the safety engineer. The program safety requirements will be stated in the contract and will require the element assembly operations to be approved by the appropriate safety authority. The safety plans will address system and facility safety requirements.</li></ul>
3.A.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for mechanical/structural damage that could cause contamination during element testing, the safety engineer will assure that appropriate safety measures are known and in place.</li></ul>

- 3.A.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that an integration process has potential for structural/mechanical damage that could cause contamination, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.A.7.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for structural/mechanical damage that could cause contamination during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.A.8.1 (prelaunch services) - No design impact during feasibility study. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 3.A.9.1 (countdown) - No design impact during feasibility study. LH2 will be loaded during countdown and structural/mechanical damage could cause contamination which could be a safety hazard.
- 3.A.10.1 (flight phase I) - No design impact during feasibility study. Launch loads could cause contamination from structural/mechanical damage and create a safety hazard.
- 3.A.11.1 (flight phase II) - No design impact during feasibility study. Launch loads could cause contamination from structural/mechanical damage and create a safety hazard.
- 3.A.12.1 (payload separation) - No design impact during feasibility study. The shock form payload separation could cause contamination from structural/mechanical damage and create a safety hazard.

Author's notes: How can the Structural/Mechanical system cause Contamination during \_\_\_\_\_ Operational Phase?

Residual contamination from manufacturing, such as metal chips or fretting of components during use, are potential safety hazards. The particles can short electrical/electronics components or lodge in valve seats to create a potential safety hazard. Some elements may react with contaminants upon contact and therefore those reactive combinations must be known and prevented. An example of this is when hydrazine (N2H4) contacts oxides. For the feasibility study, a general understanding of the effects of contaminants is necessary to assure that the potential for problems can be eliminated during the remainder of the program.

## HAZARD DEFINITIONS

3. ; B.

How can Hazardous Materials cause Contamination during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
3.B.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There are many ways that contamination can result from hazardous materials during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
3.B.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements and the training of personnel in the proper handling of hazardous materials.</li></ul>
3.B.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards and the potential for contamination that is associated with each material.</li></ul>
3.B.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. When hazardous materials are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent contamination. The potential for hazards will be reported to NASA via safety plans.</li></ul>
3.B.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test will include the use of a potentially hazardous material that could cause contamination, the safety engineer will perform an evaluation of the operation and determine the need for safety controls. They will then assure that appropriate safety measures are known and in place.</li></ul>

3.B.6.1 (system integration)

- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that an hazardous material may have the potential for contamination during system integration, the safety engineer will perform an evaluation of the operation and determine the need for safety controls. They will then assure that the appropriate controls are known and verify their effectiveness.

3.B.7.1 (system test)

- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test will involve hazardous materials with the potential for contamination, the safety engineer will perform an evaluation of the operation and determine the need for safety controls. They will then assure that the appropriate controls are known and verify their effectiveness.

3.B.8.1 (prelaunch services)

\* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. For mission unique activities that involve hazardous materials, the safety engineer will perform an evaluation to determine the potential for contamination. Upon determination that the potential for a hazardous situation exists, the safety engineer will assure that there are adequate controls in place to reduce the hazards to an acceptable level and will verify that they are effective.

3.B.9.1 (countdown)

\* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. For mission unique activities that involve hazardous materials, the safety engineer will perform an evaluation to determine the potential for contamination. Upon determination that the potential for a hazardous situation exists, the safety engineer will assure that there are adequate controls in place to reduce the hazards to an acceptable level and will verify that they are effective.

3.B.10.1 (flight phase I)

+ Not applicable: this phase does not apply to the cause category/hazard group. Contamination caused by hazardous materials is not a concern during flight because the contamination will not contact humans or render components inoperative.

3.B.11.1 (flight phase II)

+ Not applicable: this phase does not apply to the cause category/hazard group. Contamination caused by hazardous materials is not a concern during flight because the contamination will not contact humans or render components inoperative.

3.B.12.1 (payload separation) + Not applicable: this phase does not apply to the cause category/hazard group. Contamination caused by hazardous materials is not a concern during payload separation because the contamination will not contact humans or render components inoperative.

Author's notes: How can Hazardous Materials cause Contamination during \_\_\_\_\_ Operational Phase?

Hazardous materials that will be associated with COLD-SAT, such as LH2/GH2, N2H4, components or by-products of batteries, or solvents used in processing, could cause contamination. The potential for contamination by hazardous materials will be controlled by handling procedures and the training of personnel. The facility safety organizations will be relied upon to provide the assurance necessary to prevent a mishap during the use of the hazardous materials.



## HAZARD DEFINITIONS

3. ; C.

How can Environmental conditions cause Contamination during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
3.C.1.1 (launch site mods.)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There are many ways that environmental conditions can cause corrosion during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.
3.C.2.1 (subsystem mfg.)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
3.C.3.1 (transportation)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The environmental conditions during transportation will require special considerations. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. These transportation plans will be reviewed and approved by a project safety authority.
3.C.4.1 (element assembly)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Contamination resulting from environmental conditions could be introduced during element assembly. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. It will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the introduction of contaminants during element assembly.
3.C.5.1 (element test)	- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that could cause contamination, the safety engineer will assure that appropriate safety measures are known and in place.

- 3.C.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for an environmental conditions that could cause contamination, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.C.7.1 (system test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for an environmental condition that could cause contamination during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.C.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Many systems will be opened and exposed to the environment during prelaunch servicing. These operations need to be performed by experienced personnel and require adherence to approved procedures. The equipment designs need to include safeguards to prevent the introduction of contaminants during prelaunch services. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.
- 3.C.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of environmental conditions during countdown, such as filling the LH2 tank and the cold gas purge in the nose faring. Contamination could be introduced through any of the environmental condition. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.
- 3.C.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as G-loading, shock and vibration, and depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.
- 3.C.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as G-loading, shock and vibration, and depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.

3.C.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as G-loading, shock and vibration, and depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.

Author's notes: How can Environmental conditions cause Contamination during \_\_\_\_\_ Operational Phase?

Environmental conditions are: shock/vibration; G-loading; zero-G; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; etc. The results of these environmental conditions can create the potential for contamination that could result in a catastrophic failure.

This analysis will evaluate the potential for something to become contaminated by an environmental condition. An example is rain entering an electrical connector causing shorts or corrosion, air combining with a purge gas causing liquid air to form in the MLI, or particles entering a system where they could cause physical damage.

## **HAZARD DEFINITIONS**

3. ; D.

How can Pneumatics cause Contamination or become Contaminated during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
3.D.1.1 (launch site mods.)	- No design impact during feasibility study. During site modifications involving pneumatic systems, the standard facility safety requirements and systems will be relied upon for control, including the requirements of ESMCR 127-1, chapter 5.
3.D.2.1 (subsystem mfg.)	- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements including any potential for pneumatics causing contamination that would create a safety hazard.
3.D.3.1 (transportation)	- No design impact during feasibility study. Currently, it can not be conceived how pneumatics can cause contamination during transportation of components, assemblies, or the satellite.
3.D.4.1 (element assembly)	- No design impact during feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be written into the procedures.
3.D.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test involves pneumatics that have the potential for causing contamination that could cause a safety hazard, the appropriate safety authority will assure that appropriate safety controls are in place to reduce the hazard to an acceptable level.
3.D.6.1 (system integration)	* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.7.1 (system test)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.10.1 (flight phase I)

- No design impact during feasibility study. The pneumatic systems will be sealed during flight phase I and the clean gases and filters will have been included in the design for the earlier program phases.

3.D.11.1 (flight phase II)

- No design impact during feasibility study. The pneumatic systems will be sealed during flight phase I and the clean gases and filters will have been included in the design for the earlier program phases.

3.D.12.1 (payload separation)

- No design impact during feasibility study. The pneumatic systems will be sealed during flight phase I and the clean gases and filters will have been included in the design for the earlier program phases.

Author's notes: How can Pneumatics cause Contamination or become Contaminated during \_\_\_\_\_ Operational Phase?

The pneumatics can cause contamination of components or systems or the pneumatic system can be contaminated by components or systems.

## **HAZARD DEFINITIONS**

3. ; E.

**How can the Electrical/Electronics system cause Contamination or how can the Electronics become Contaminated during \_\_\_\_\_ Operational Phase?**

<b>CODE</b>	<b>DESCRIPTION</b>
3.E.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The electrical/electronics systems on the launch site could become contaminated during normal launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
3.E.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. During the subsystems manufacturing there will be many opportunities for items to become contaminated that could result in a potential safety hazard. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will evaluate the potential for electrical/electronics to become contaminated.</li></ul>
3.E.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. The transportation of electrical/electronics will offer many opportunities for contamination. System safety will evaluate the transportation plans to determine if there is the potential for contamination that could result in potential hazards.</li></ul>
3.E.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be evaluated by a safety engineer and appropriate safety controls will be included in the procedures. When electrical/electronics have the potential for contamination that could result in a potential hazard, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the potential hazard. The potential for hazards will be reported to NASA via safety plans.</li></ul>

- 3.E.5.1 (element test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for electrical/electronics to become contaminated and to create a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.E.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has the potential for contaminating electrical/electronics and create a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.E.7.1 (system test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has the potential for electrical/electronics to become contaminated and result in a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.E.8.1 (prelaunch services)
- \* This could be a design impact that should be considered during the preliminary design. Preluanch servicing will require electrical/electronics to be installed/removed which could provide an opportunity for contamination. The impact of the contamination will be evaluated by the program system safety authority for their potential safety hazards. Upon determination that there is a potential safety impact, the system safety authority will assure that the appropriate safety measures are incorporated.
- 3.E.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. During countdown the electrical/electronics on board the spacecraft will be exposed to controlled environmental purge which is a design parameter for the electrical/electronics equipment. The GSE electrical/electronics equipment will be exposed to adverse environments that will also be included in the design requirements. The project system safety engineer will evaluate the design requirements and the designs to assure that they are adequate to preclude any potential hazards from electrical/electronics being contaminated.
- 3.E.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. Depressurization upon ascent could cause out gassing resulting in contamination. The project approved materials list will indicate materials that have the potential for out gassing. System safety will verify that there are adequate design requirements to preclude out gassing that could result in a potential hazard.

3.E.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. Depressurization upon ascent could cause out gassing resulting in contamination. The project approved materials list will indicate materials that have the potential for out gassing. System safety will verify that there are adequate design requirements to preclude out gassing that could result in a potential hazard.

3.E.12.1 (payload separation) - No design impact during feasibility study. It currently can not be conceived how electrical/electronics can become contaminated or cause contamination during payload separation.

Author's notes: How can the Electrical/Electronics system cause Contamination or how can the Electronics become Contaminated during \_\_\_\_\_ Operational Phase?

Substances causing contamination and the receiver of contamination will be addressed by this analysis.

Contamination is a foreign material(s) that has an adverse effect(s), such as air in a nitrogen purged atmosphere or metal chips in an electrical unit. Electrical/electronics do not produce contamination. Hermetically sealed electrical/electronics units that have defective seals could become contaminated with air or other gas. A non-sealed unit could become contaminated if they were exposed to a contaminating environment.

Environmental conditions cause contamination (3.C) addresses the contamination of electronics by environments such as salt air or a contaminated purge gas.

Environmental conditions cause electrical shock/shorts addresses conductive particles contamination the electrical/electronics equipment.

An electrical charge or a noisy electrical signal could be considered as a type of contamination to an electrical unit, but this **type** of electrical contamination will not be considered as part of the analysis.



## HAZARD DEFINITIONS

3. ; F.

**How can Ordnance cause Contamination or how can Ordnance become Contaminated during Operational Phase ?**

CODE	DESCRIPTION
3.F.1.1 (launch site mods.)	+ Not applicable: this phase does not apply to the cause category/hazard group. It can not be conceived how ordnance would be used during launch site modifications.
3.F.2.1 (subsystem mfg.)	- No design impact for feasibility study. Active ordnance that could cause contamination are not normally involved in subsystem manufacturing. The safety associated with the manufacturing of ordnance devices will be the responsibility of the manufacturer. Ordnance are normally procured as complete devices that are installed as units on the spacecraft. Therefore, the project will only be concerned upon receipt and installation of ordnance. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
3.F.3.1 (transportation)	- No design impact for feasibility study. Ordnance could be transported after installation onto the satellite, if they are installed in a processing facility prior to moving it to the launch site. Normally, ordnance are not armed until late in the processing, at final closeout of the satellite. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards and the potential effects, such as contamination, that are associated with each material.
3.F.4.1 (element assembly)	+ Not applicable: this phase does not apply to the cause category/hazard group. Normally, ordnance are not installed or used during element assembly. This analysis only addresses the ordnance after they are received from the supplier. Element assembly will occur at the supplier's facility.
3.F.5.1 (element test)	- No design impact during feasibility study. Ordnance may be used during element tests. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has the potential for ordnance causing contamination or ordnance becoming contaminated, the safety engineer will assure that appropriate safety measures are known and in place.

- 3.F.6.1 (system integration)
- No design impact during feasibility study. System integration would not normally include the use of ordnance. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that an integration process has potential for ordnance to cause contamination or become contaminated and result in a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place in order to reduce the potential hazard to an acceptable level.
- 3.F.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for ordnance to cause contamination or become contaminated and result in a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place in order to reduce the potential hazard to an acceptable level.
- 3.F.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Ordnance will be included in prelaunch servicing operations. When specifying the type of ordnance during the design phases, the handling and installation methods need to be considered for their safety impacts. System safety will assist in determining proper methods for handling, installing, and arming ordnance during prelaunch servicing.
- 3.F.9.1 (countdown)
- No design impact during feasibility study. It currently can not be conceived how contamination could cause a potential hazard during countdown.
- 3.F.10.1 (flight phase I)
- No design impact during feasibility study. It currently can not be conceived how contamination could cause a potential hazard during flight.
- 3.F.11.1 (flight phase II)
- No design impact during feasibility study. It currently can not be conceived how contamination could cause a potential hazard during flight.

3.F.12.1 (payload separation) - No design impact during feasibility study. It currently can not be conceived how contamination could cause a potential hazard during payload separation.

Author's notes: How can Ordnance cause Contamination or how can Ordnance become Contaminated during Operational Phase ? \_\_\_\_\_

This analysis will only address ordnance upon receipt at the point of installation. Ordnance could become contaminated during manufacturing, assembly, transportation, installation or other handling processes. Normally, the manufacturing, assembly, packaging and handling of space flight hardware is very well controlled by the use of procedures and special packaging.

The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments; they are all self-contained in their housings. Ordnance are usually installed during prelaunch services either at the hazardous processing facility or at the launch pad.

A band clamp type separation system is currently being proposed for COLD-SAT. This system has frangible bolts that are self-contained and will not produce high energy fragments or contamination.

## HAZARD DEFINITIONS

3. ; G.

How can Propulsion cause Contamination during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
3.G.1.1.1 (launch site mods.)	+ Not applicable: this phase does not apply to the cause category/hazard group. Currently, it can not be conceived how any propulsive elements are associated with the site modifications.
3.G.2.1 (subsystem mfg.)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There will be many opportunities for the propulsion system to become contaminated during subsystem manufacturing that could result in a potential safety hazard. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
3.G.3.1 (transportation)	- No design impact for feasibility study. The transportation of the propulsion system as a subassembly, assembled system, or after N2H4 tanking will provide many opportunities for contamination either to the system or by the system. The potential for N2H4 to cause contamination is addressed in 2.B, Contamination of Hazardous Materials. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address the potential for contamination of or by the propulsive system will be included in the transportation plans. These transportation plans will be reviewed and approved by a project safety authority.
3.G.4.1 (element assembly)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When propulsive elements are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent contamination. The potential for hazards will be reported to NASA via safety plans.

- 3.G.5.1 (element test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for a propulsive element to cause contamination during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.G.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. There will be many opportunities for the propulsion system to become contaminated during system integration. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for contamination that could cause a potential safety hazard during system integration the system safety engineer will assure that appropriate safety measures are known and in place.
- 3.G.7.1 (system test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for propulsion that could cause contamination during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 3.G.8.1 (prelaunch services)
- \* This could be a design impact that should be considered during the preliminary design. The hydrazine will be loaded during prelaunch servicing which provides an opportunity for the system to become contaminated. This contamination could be a potential safety hazard. The preliminary design should include adequate filters in the loading and on-board systems.
- 3.G.9.1 (countdown)
- No design impact during feasibility study. The propulsive system will be sealed during countdown and will not be active and therefore will not cause contamination or become contaminated. The current feasibility study design incorporates two barriers in the fill/drain line to guard against external leakage and two barriers between the N2H4 and the thruster catalyst beds.
- 3.G.10.1 (flight phase I)
- No design impact during feasibility study. The propulsive system will be sealed during flight and will not be active and therefore will not cause contamination or become contaminated. The current design provides two barriers between the N2H4 and the catalyst beds of the thrusters which is adequate protection to prevent contamination by unplanned thruster firing.

3.G.11.1 (flight phase II)

- No design impact during feasibility study. The propulsive system will be sealed during flight and will not be active and therefore will not cause contamination or become contaminated. The current design provides two barriers between the N2H4 and the catalyst beds of the thrusters which is adequate protection to prevent contamination by unplanned thruster firing.

3.G.12.1 (payload separation) - No design impact during feasibility study. The propulsive system will be sealed during flight and will not be active and therefore will not cause contamination or become contaminated. The current design provides two barriers between the N2H4 and the catalyst beds of the thrusters which is adequate protection to prevent contamination by unplanned thruster firing.

Author's notes: How can Propulsion cause Contamination during \_\_\_\_\_ Operational Phase?

The products or results of propulsion may include: thrust, heat, combustion and/or by-products of combustion.

Substances causing contamination and the receiver of contamination will be addressed by this analysis. Contamination is a foreign material(s) that has an adverse effect(s), such as the by-products of spent N2H4 depositing on optical surfaces.

The only propulsive element planned for COLD-SAT is the hydrazine thrusters for reaction control and induced thrust for experimentation. The hydrogen vent system may produce a propulsive thrust which is very slight. The expelled hydrogen could cause contamination concerns.

## HAZARD DEFINITIONS

3. ; H.

How can Non-Ionizing Radiation cause Contamination during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how non-ionizing radiation can cause contamination during any of the operational phases.

Author's notes: How can Non-Ionizing Radiation cause Contamination during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves. The level of non-ionizing radiation from the spacecraft antenna is very low and is very unlikely to cause injury to personnel. The communication GSE where high energy radio waves are used is not included in this analysis.

## **HAZARD DEFINITIONS**

3. ; I.

How can Ground Support Equipment cause Contamination during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
3.I.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Currently, it can not be conceived how the Ground Support Equipment could cause Contamination or become contaminated and create a potential hazard during launch site modifications. There will be many opportunities for contamination both to and by GSE during launch site modifications. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts.</li></ul>
3.I.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements including the potential for GSE to cause or become contaminated and create a potential hazard.</li></ul>
3.I.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly including GSE will be stated in the requirements documentation. There will be many opportunities for GSE to become contaminated during transportation. System Safety will review the transportation plans and evaluate the potential for contamination to create a potential hazard. Upon determination that there is the potential for contamination that poses a hazard, the system safety engineer will assure that appropriate safety measures are known and in place.</li></ul>
3.I.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all major GSE assemblies. The system safety engineer will evaluate the assembly of the GSE for its potential hazards including the impact of contamination. Upon determination that there is the potential for contamination that poses a hazard, the system safety engineer will assure that appropriate safety measures are known and in place.</li></ul>



3.I.5.1 (element test)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The introduction of contaminants that could cause potential safety hazards will be evaluated by the system safety engineer. Test plans/procedures will be required for all testing. Upon determination that a test of GSE has potential for contamination that could create a potential hazard, the safety engineer will assure that appropriate safety measures are known and in place.

3.I.6.1 (system integration)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider the integration of GSE for potential safety impacts. Upon determination that there is the potential for a hazard resulting from the contamination of GSE, the safety engineer will assure that appropriate safety measures are known and in place.

3.I.7.1 (system test)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for introducing contaminants that could create the potential for a hazard during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.

3.I.8.1 (prelaunch services)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. GSE will be used extensively during prelaunch servicing and there will be many opportunities to introduce contamination. System safety will evaluate the use of GSE to determine the potential hazards associated with each operation.

3.I.9.1 (countdown)

+ Not applicable: this phase does not apply to the cause category/hazard group.

3.I.10.1 (flight phase I)

+ Not applicable: this phase does not apply to the cause category/hazard group.

3.I.11.1 (flight phase II)

+ Not applicable: this phase does not apply to the cause category/hazard group.

3.I.12.1 (payload separation) + Not applicable: this phase does not apply to the cause category/hazard group.

Author's notes: How can Ground Support Equipment cause Contamination during \_\_\_\_\_ Operational Phase?

Contamination by itself does not pose a potential hazard. The results of the contamination must be evaluated to determine the potential for a safety hazard.

## HAZARD DEFINITIONS

### 4. ; A.

How can the Structural/Mechanical system cause an Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

Currently, it can not be conceived how Structural/Mechanical cause Electrical shock/shorts during any of the Operational Phases.

This issue will be re-evaluated during each phase of the program in an effort to determine if any potential hazards can be identified.

Author's notes: How can the Structural/Mechanical system cause an Electrical Shock/Short during \_\_\_\_\_ Operational Phase?

88

A structural/mechanical item by itself can not cause an electrical shock/short because they do not produce or carry electrical potential.

A failure of a structural/mechanical item could create a short. The structural/mechanical designs will contain adequate margins of safety to prevent failures. System safety will rely on the design and verification systems to assure that mechanical/structural items will not fail and cause electrical shorts/shocks. System safety will evaluate the designs at a system level to determine the potential for electrical shorts/shocks.

## **HAZARD DEFINITIONS**

4. ; B.

How can Hazardous Materials cause Electrical Shock during \_\_\_\_\_ Operational Phase?

**CODE**

**DESCRIPTION**

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Hazardous Materials can cause Electrical Shock/shorts during any of the operational phases.

Author's notes: How can Hazardous Materials cause Electrical Shock during \_\_\_\_\_ Operational Phase?

Hazardous materials that will be associated with COLD-SAT are LH2/GH2, N2H4, components or by-products of batteries, or solvents used in processing. The facility safety organizations will be relied upon to provide the assurance necessary to prevent a mishap during the use of the hazardous materials. A project approved materials list will be compiled. It will include the hazards or hazardous conditions for each material that will be used on the project. Methods for controlling these hazardous materials will be considered during the preliminary design phase of the program.

## HAZARD DEFINITIONS

### 4. ; C.

How can Environmental conditions cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
4.C.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There are many ways that electrical shock could result from environmental conditions during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
4.C.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements.</li></ul>
4.C.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address electrical shock caused by environmental conditions will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.</li></ul>
4.C.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When environmental conditions create a potential for electrical shock during element assembly, it will be the responsibility of the organization that is performing the operation to assure that adequate controls are in-place to reduce the potential to an acceptable level.</li></ul>
4.C.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that could cause electrical shock during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</li></ul>
4.C.6.1 (system integration)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for environmental conditions that could cause electrical shock, the safety engineer will assure that appropriate safety measures are known and in place.</li></ul>

#### 4.C.7.1 (system test)

- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that could cause electrical shock during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.

#### 4.C.8.1 (prelaunch services)

- No design impact during feasibility study. Pad/area safety plans and the review of the safety plans will be relied upon to identify environmental conditions that create the potential for electrical shock. Many of these considerations are addressed in ESMCR 127-1.

#### 4.C.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. LH2 is being tanked during countdown which creates the potential for temperature extremes and condensation. The preliminary design should consider the effects of these conditions on the electrical equipment.

#### 4.C.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The most severe shock and vibration conditions and liquid air run-off conditions occur at flight phase I. These conditions need to be considered in the design phase of development and methods to prevent electrical shock need to be considered.

#### 4.C.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. Very severe shock and vibration conditions and liquid air run-off conditions occur at flight phase II. These conditions need to be considered in the design phase of development and methods to prevent electrical shock.

#### 4.C.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The separation system creates a shock when it is activated and needs to be considered during the preliminary design for its potential for creating electrical shock.

Author's notes: How can Environmental conditions cause Electrical Shock during \_\_\_\_\_ Operational Phase?

Environmental conditions are: shock/vibration; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; etc. The results of these environmental conditions can create the potential for hazards such as electrical shock to personnel. Condensation, rain or other sources of moisture can provide a conductive path. Current limiting devices are used to reduce the probability of injury to personnel or damage to equipment.

## HAZARD DEFINITIONS

4. ; D.

How can Pneumatics cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Pneumatics can cause Electrical Shock during any of the operational phases.

Author's notes: How can Pneumatics cause Electrical Shock during \_\_\_\_\_ Operational Phase?

The pressurization system for COLD-SAT will use GH2 and GHE. The GH2 and GHE will be loaded on the ground. GH2 will also be generated, on-orbit, from LH2. GN2, compressed air, compressed O2 or other pressurants may be used for ground operations.

## HAZARD DEFINITIONS

4. ; E.

How can the Electrical/Electronics system cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
4.E.1.1 (launch site mods.)	- No design impact for feasibility study. There are many ways that the electrical/electronics could cause electrical shock during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.
4.E.2.1 (subsystem mfg.)	- No design impact during feasibility study. System safety will review the subsystem designs to evaluate the potential for electrical shock and, upon identification of that potential, will work with the designers to reduce the risk to an acceptable level. The subsystem manufacturers will be required to have a NASA approved system safety plan that will address electrical shock hazards.
4.E.3.1 (transportation)	- No design impact during feasibility study. Any transportation of electronics/electronics either as components, assemblies, or after integration will be considered during the design for the potential of electrical shock. In cases where the hazards can not be eliminated or reduced to an acceptable level, proper handling will be controlled by the procedures.
4.E.4.1 (element assembly)	- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When the potential for electrical shock is evident, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent electrical shock. The potential for hazards will be reported to NASA via safety plans.
4.E.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that there is a potential for electrical shock during an element test, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.
4.E.6.1 (system integration)	* This could be a design impact that should be considered during the preliminary design. During system integration there will be many operations concerning electrical/electronics. The preliminary design should consider the integration methods and reduce the potential for electrical shock in the design.

- 4.E.7.1 (system test)
- \* This could be a design impact that should be considered during the preliminary design. During system testing there will be many opportunities for electrical shock from electrical/electronics. The preliminary design should consider testing methods and reduce the potential for electrical shock in the design.
- 4.E.8.1 (prelaunch services)
- \* This could be a design impact that should be considered during the preliminary design. During prelaunch services there will be many opportunities for electrical shock from electrical/electronics. The preliminary design should consider servicing methods and reduce the potential for electrical shock in the design.
- 4.E.9.1 (countdown)
- No design impact during feasibility study. During countdown the electronics/electronics will not be stressed. In preparation for launch it will be verified that they are ready and electrical shock should not be a concern.
- 4.E.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. During flight phase I, the greatest amount of stress and vibration will normally occur. The designers should consider the flight loads when specifying the electrical/electronics so they will be robust enough to withstand the launch environments.
- 4.E.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. During flight phase II, a significant amount of stress and vibration will occur. The designers should consider the flight loads when specifying the electrical/electronics so they will be robust enough to withstand the launch environments.
- 4.E.12.1 (payload separation)
- \* This could be a design impact that should be considered during the preliminary design. There are some unique shock loads encountered during payload separation. The system designer needs to consider these loads and their effects on specific electronics/electrical components during preliminary design so that the risk of electrical shocks/shorts can be minimized.

Author's notes: How can the Electrical/Electronics system cause Electrical Shock during \_\_\_\_\_ Operational Phase?



## HAZARD DEFINITIONS

4. ; F.

How can Ordnance cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
4.F.1.1 (launch site mods.)	+ Not applicable: this phase does not apply to the cause category/hazard group. Ordnance are not normally associated with the launch site modifications.
4.F.2.1 (subsystem mfg.)	- No design impact for feasibility study. The safety associated with the manufacturing of ordnance devices will be the responsibility of the manufacturer. This includes the potential for ordnance to cause electrical shock/shorts. Ordnance are normally procured as complete devices that are installed as units on the spacecraft. Therefore, the project will only be concerned upon receipt and installation of ordnance. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
4.F.3.1 (transportation)	- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials including ordnance. The "program hazardous materials list" will be used to identify the hazards and their potential effects that are associated with each material. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation.
4.F.4.1 (element assembly)	- No design impact for feasibility study. The assembly of ordnance is the responsibility of the supplier of the ordnance. The assembly of the ordnance into the satellite will be performed using written procedures. Ordnance are not normally a part of element assembly. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When ordnance are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the potential for electrical shocks/shorts. The potential for hazards will be reported to NASA via safety plans.

- 4.F.5.1 (element test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for ordnance to cause electrical shock/shorts during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 4.F.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Normally, ordnance is not included in system integration. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for ordnance that could cause electrical shock/shorts, the safety engineer will assure that appropriate safety measures are known and in place.
- 4.F.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for ordnance to cause electrical shorts or shocks, the safety engineer will assure that appropriate safety measures are known and in place.
- 4.F.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Ordnance will be installed and possibly armed during prelaunch services. The potential for electrical shocks/shorts will be evaluated by the system safety engineer during preliminary design and the system safety engineer will work with the design engineers to incorporate the appropriate design features to reduce the potential hazard to an acceptable level.
- 4.F.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. The ordnance may be armed during countdown. Procedures will be used for all operations during countdown and system safety will review all procedures to identify any potential safety impacts. The potential for other hazards concerning ordnance and electrical shocks/shorts will be evaluated by the system safety engineer.
- 4.F.10.1 (flight phase I)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System safety will evaluate the preliminary design to determine if there is a potential for ordnance to cause electrical shock/shorts during flight.
- 4.F.11.1 (flight phase II)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System safety will evaluate the preliminary design to determine if there is a potential for ordnance to cause electrical shock/shorts during flight.

4.F.12.1 (payload separation) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System safety will evaluate the preliminary design to determine if there is a potential for ordnance to cause electrical shock/shorts during payload separation.

Author's notes: How can Ordnance cause Electrical Shock during \_\_\_\_\_ Operational Phase?

Ordnance do not generate electric power and therefore can not cause electrical shock. Ordnance use electrical power to activate. Normally, the electrical power is not connected to the ordnance until just prior to launch countdown. Also, normally, the ordnance are checked for shorts after installation on the satellite.

The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments; they are all self-contained in their housings. Ordnance are usually installed during prelaunch services either at the hazardous processing facility or at the launch pad.

A band clamp type separation system is currently being proposed for COLD-SAT. This system has frangible bolts that are self-contained and will not produce high energy fragments or contamination.

The primary hazard for electrical shock/short is injury to personnel either by direct contact or by the results of the shock/short.

9 Ordnance are activated by sending an electrical signals to an initiator. If a short were to occur that sent a  
3 unplanned signal, the results could be a potential hazard.

## HAZARD DEFINITIONS

4. ; G.

How can Propulsion cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Propulsion can cause Electrical Shock during any of the operational phases.

Author's notes: How can Propulsion cause Electrical Shock during \_\_\_\_\_ Operational Phase?

Propulsion includes any system that has the potential for causing propulsion, it is not restricted to the propulsion system. The COLD-SAT propulsion system will have isolation valves to prevent N2H4 from entering the thruster loop until after t-0. Redundant thruster valving will prevent the N2H4 from entering the REMs until the valves are commanded open.

If a propulsive element were to be activated inadvertently, it could cause damage to electrical equipment and possibly cause electrical shock/shorts. This is a second order failure which is beyond the scope of this analysis.

## HAZARD DEFINITIONS

4. ; H.

How can Non-Ionizing Radiation cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how non-ionizing radiation can cause electrical shock during any of the operational phases.

Author's notes: How can Non-Ionizing Radiation cause Electrical Shock during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves. The level of non-ionizing radiation from the spacecraft antenna is very low and is very unlikely to cause injury to personnel. The communication GSE where high energy radio waves are used is not included in this analysis.

## **HAZARD DEFINITIONS**

4. ; I.

How can Ground Support Equipment cause Electrical Shock during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
4.I.1.1 (launch site mods.)	<p>* This could be a design impact and should be considered during preliminary design. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The launch site is considered GSE and there will be many uses of electrical power on the launch site. System safety will evaluate the proposed launch site modifications during preliminary design to determine the potential for electrical shocks/shorts during any operation.</p> <p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</p>
4.I.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address electrical shocks/shorts caused by GSE will be evaluated by the system safety authority who will assure that the appropriate safety requirements are known and incorporated.</p>
4.I.3.1 (transportation)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When a potential hazard is identified concerning electrical shocks/shorts from GSE, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the hazard from occurring. The potential for hazards will be reported to NASA via safety plans.</p>
4.I.4.1 (element assembly)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When a potential hazard is identified concerning electrical shocks/shorts from GSE, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the hazard from occurring. The potential for hazards will be reported to NASA via safety plans.</p>

4.I.5.1 (element test)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test involving GSE has potential for electrical shocks/shorts, the safety engineer will assure that appropriate safety measures are known and in place.

4.I.6.1 (system integration)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for GSE to cause an electrical shock/short, the safety engineer will assure that appropriate safety measures are known and in place.

4.I.7.1 (system test)

- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all major testing of GSE. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for GSE to cause electrical shocks/shorts, the safety engineer will assure that appropriate safety measures are known and in place.

4.I.8.1 (prelaunch services)

\* This could be a design impact and should be considered during preliminary design. GSE will be used extensively during prelaunch servicing. System safety will evaluate the GSE and its use during prelaunch servicing to determine any potential for electrical shocks/shorts.

4.I.9.1 (countdown)

\* This could be a design impact and should be considered during preliminary design. GSE will be used extensively during countdown. System safety will evaluate the GSE and its use during countdown to determine any potential for electrical shocks/shorts.

4.I.10.1 (flight phase I)

+ Not applicable: this phase does not apply to the cause category/hazard group.

4.I.11.1 (flight phase II)

+ Not applicable: this phase does not apply to the cause category/hazard group.

4.I.12.1 (payload separation)

+ Not applicable: this phase does not apply to the cause category/hazard group.

Author's notes: How can Ground Support Equipment cause Electrical Shock during \_\_\_\_\_ Operational Phase?

GSE will utilize electrical power extensively for control and operations. Both AC and DC power are used for GSE. At the feasibility study phase of the program the GSE is not well defined except for functional applications such as the loading of LH2 and N2H4.

Electrical shocks and shorts can have several hazardous results such as injury to personnel or as an ignition source for fire or explosion.

## HAZARD DEFINITIONS

5. ; A.

How can the Structural/Mechanical system cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Structural/Mechanical items can cause fire during any of the operational phases. Structural/mechanical items are normally neither an ignition source nor will they support combustion and therefore is not a potential fire hazard.

Author's notes: How can the Structural/Mechanical system cause Fire during \_\_\_\_\_ Operational Phase?

Fire is caused by a combination of combustible material and an ignition source. The medium used for structural/mechanical items is normally neither a combustible nor an ignition source. The fracturing of a structural/mechanical item could cause a spark or rupture a vessel containing a flammable medium. These are second order failures and the first order failures are addressed elsewhere in the hazard matrix.



## HAZARD DEFINITIONS

5. ; B.

How can Hazardous Materials cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.B.1.1 (launch site mods.)	<p>- No design impact during feasibility study. The standard facility safety requirements and systems will be relied upon to control site modifications. There are many hazardous materials, such as solvents or cleaning agents that will be used during site modifications. Their uses can not be considered during the preliminary design phase.</p>
5.B.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. It will be the responsibility of the manufacturers of the subsystems to assure the safety of the hardware and personnel, which includes fire from hazardous materials. All subsystem manufacturers will be required to have a NASA approved safety plan, per their contract. The potential for using hazardous materials that could cause fire will be identified and addressed in this plan.</p>
5.B.3.1 (transportation)	<p>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards that are associated with each material.</p>
5.B.4.1 (element assembly)	<p>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When hazardous materials are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent explosions. The potential for hazards will be reported to NASA via safety plans.</p>
5.B.5.1 (element test)	<p>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for the use of hazardous materials that could cause fire. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. Upon determination that a test has potential for explosion from hazardous materials during the element tests, the system engineer will assure that appropriate safety measures are known and in place.</p>

- 5.B.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for a fire due to hazardous materials during system integration, the safety engineer will assure that appropriate safety measures are known and in place.
- 5.B.7.1 (system test)
- \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. All system tests using LH2/GH2 need to be considered for methods to reduce their hazards during the feasibility study.
- 5.B.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. The primary hazardous material that has the potential for causing fire during prelaunch services is LH2/GH2.
- 5.B.9.1 (countdown)
- \* This could be a design impact that should be considered during preliminary design. Systems for the proper venting of GH2 during countdown may have a design impact and need to be considered during the preliminary design. The other hazardous materials that have the potential for causing fire need to be reviewed for potential design impacts.
- 5.B.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. During flight phase I the greatest amount of stress and vibration will normally occur. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary for their potential safety impacts.
- 5.B.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

5.B.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. Payload separation involves a shock factor and an ignition source. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

Author's notes: How can Hazardous Materials cause Fire during \_\_\_\_\_ Operational Phase?

Hazardous materials need to be controlled. They can be in a solid, liquid or gaseous state or a combination of these states. A project approved materials list will be compiled. It will include the hazards or hazardous conditions for each material that will be used on the project. Methods for controlling these hazardous materials will be considered during the preliminary design phase of the program.

The currently known hazardous materials that are associated with COLD-SAT are LH2/GH2, N2H4, components or by-products of batteries, or solvents used in processing. The facility safety organizations will be relied upon to provide the assurance necessary to prevent a mishap during the use of the hazardous materials.

## HAZARD DEFINITIONS

5. ; C.

How can Environmental conditions cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts for any of the Operational Phases. At the feasibility phase of the program it can not be conceived how environmental conditions could contribute to a fire, except for those that are addressed in other sections of this hazard analysis.

Author's notes: How can Environmental conditions cause Fire during \_\_\_\_\_ Operational Phase?

Fire is caused by a combination of a combustible material and an ignition source.

Environmental conditions are: shock/vibration; G-loading; zero-G; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; lightning; etc.

Environmental conditions that could be considered ignition sources are: ESD (electrostatic discharge) or lightning.

At the feasibility phase of the COLD-SAT program, the known combustible materials are LH2/GH2 and N2H4 and possibly foam insulation. The potential fire hazards for LH2/GH2 and N2H4 are addressed in 5.B., Hazardous Materials cause Fires. This includes a flammable atmosphere resulting from a hydrogen leak.

All materials proposed for use on the COLD-SAT program, including the foam insulation, will be included on the project approved materials list. As this list is being compiled, system safety will evaluate these materials for their potential for contributing to a fire hazard.

## HAZARD DEFINITIONS

5. ; D.

How can Pneumatics cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.D.1.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There are many ways that pneumatics could provide the fuel for a fire if they are combustible. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li> </ul>
5.D.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li> </ul>
5.D.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials including pneumatics that are flammable. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards and the potential effects, that are associated with each material.</li> </ul>
5.D.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When combustible pneumatics are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the hazardous effects. The potential for hazards will be reported to NASA via safety plans.</li> </ul>
5.D.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing fires during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</li> </ul>
5.D.6.1 (system integration)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for pneumatics causing fires, the safety engineer will assure that appropriate safety measures are known and in place.</li> </ul>

5.D.7.1.1 (system test)

- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing fires during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.

5.D.8.1 (prelaunch services)

\* This could be a design impact and should be considered during preliminary design. GH2 is to be loaded prior to launch. This will require all electrical service in the area to be terminated or have only spark proof electrical components in use during GH2 loading. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

5.D.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during countdown. If the GH2 were to leak, it could be ignited by an electrical source of other operations during countdown.

5.D.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by an electrical source of other flight operations.

5.D.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by an electrical source of other flight operations.

5.D.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by the shape charge or an electrical source during payload separation.

Author's notes: How can Pneumatics cause Fire during \_\_\_\_\_ Operational Phase?

Fire is caused by a combination of a combustible material and an ignition source. The medium used for pneumatics could be combustible, but the medium is typically selected as non-combustible to prevent fire hazards. The pressurization system for COLD-SAT will use GH2 and GHe. The GH2 will be loaded on the ground. On orbit, GH2 will be generated from LH2. Many of the issues are covered in 5.B, Hazardous Materials causes Fires.

## HAZARD DEFINITIONS

5. ; E.

How can the Electrical/Electronics system cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.E.1.1 (launch site mods.)	<p>- No design impact for feasibility study. There are many ways that Fire can occur due to Electrical/Electronics during launch site modifications if there is a medium to support the combustion after electrical/electronics provides the ignition source. The standard facility safety requirements and systems will be relied upon to control the rapidly combustible materials during launch site modifications, including the requirements of ESMCR 127-1, chapter 5.</p>
5.E.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements including concerns with electrical/electronics providing an ignition source for combustible materials.</p>
5.E.3.1 (transportation)	<p>- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address fires caused by electrical/electronics providing the ignition source for rapidly combustible materials, will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.</p>
5.E.4.1 (element assembly)	<p>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When electrical/electronics are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to eliminate the potential for igniting a combustible material. The potential for hazards will be reported to NASA via safety plans.</p>
5.E.5.1 (element test)	<p>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for electrical/electronics that would provide an ignition source for combustible materials during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</p>

- 5.E.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has the potential for electrical/electronics that would provide an ignition source for combustible materials, the safety engineer will assure that appropriate safety measures are known and in place.
- 5.E.7.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for electrical/electronics that would provide an ignition source for combustible materials during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 5.E.8.1 (prelaunch services) \* This could be a design impact and should be considered during preliminary design. Electrical/electronics and LH2/GH2 will be present and in-uses during prelaunch services. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 5.E.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.
- 5.E.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.
- 5.E.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.
- 5.E.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.

Author's notes: How can the Electrical/Electronics system cause Fire during \_\_\_\_\_ Operational Phase?

Electrical shorts are ignition sources for fires but an electrical short is not considered a fire because it does not support the combustion. The combustion sources need to be considered for their potential for causing fires and their location in relation to the ignition sources. These considerations are not a concern during the feasibility study except for known media such as LH2/GH2.



## HAZARD DEFINITIONS

5. ; F.

How can Ordnance cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.F.1.1 (launch site mods.)	+ Not applicable: this phase does not apply to the cause category/hazard group. Ordnance is not normally involved with launch site modifications.
5.F.2.1 (subsystem mfg.)	+ Non applicable: The manufacturing of the ordnance is beyond the scope of this analysis. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
5.F.3.1 (transportation)	- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards and their effects, that are associated with each material.
5.F.4.1 (element assembly)	- No design impact for feasibility study. The assembly of the ordnance devices will be the responsibility of the manufacturers. Normally, ordnance devices are installed during prelaunch servicing and not during element assembly. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When ordnance are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the potential for fire. The potential for hazards will be reported to NASA via safety plans.
5.F.5.1 (element test)	- No design impact during feasibility study. Testing of the ordnance devices will be the responsibility of the ordnance manufacturers. Test plans/procedures will be required for all testing. If ordnance is to be used in an element test, System safety will consider the test plans for potential safety impacts. Upon determination that a test has potential for ordnance to cause fire, the safety engineer will assure that appropriate safety measures are known and in place.

- 5.F.6.1.1 (system integration) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for ordnance to cause fire, the safety engineer will assure that appropriate safety measures are known and in place.
- 5.F.7.1.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a system test has potential for ordnance to cause fire, the safety engineer will assure that appropriate safety measures are known and in place.
- 5.F.8.1.1 (prelaunch services) - No design impact during feasibility study. The ordnance devices will possibility be installed and will be armed during prelaunch services. At this point the ordnance devices will be contained on their housings and will not be a potential ignition source. During each of the program phases, system safety will review the design of the ordnance and determine if there are any potential safety hazards.
- 5.F.9.1.1 (countdown) - No design impact during feasibility study. During countdown the ordnance will be armed. If they are inadvertently activated they will not provide a potential ignition source because they are self contained. During each of the program phases, system safety will review the design of the ordnance and determine if there are any potential safety hazards.
- 5.F.10.1.1 (flight phase I) - No design impact during feasibility study. During flight the ordnance will be armed. If they are activated either intentionally or inadvertently, they will not provide a potential ignition source because they are self contained. During each of the program phases, system safety will review the design of the ordnance and determine if there are any potential safety hazards.
- 5.F.11.1.1 (flight phase II) - No design impact during feasibility study. During flight the ordnance will be armed. If they are activated either intentionally or inadvertently, they will not provide a potential ignition source because they are self contained. During each of the program phases, system safety will review the design of the ordnance and determine if there are any potential safety hazards.

5.F.12.1 (payload separation) - No design impact during feasibility study. During payload separation the ordnance will be armed. If they are activated either intentionally or inadvertently, they will not provide a potential ignition source because they are self contained. During each of the program phases, system safety will review the design of the ordnance and determine if there are any potential safety hazards.

Author's notes: How can Ordnance cause Fire during \_\_\_\_\_ Operational Phase?

Fire requires a flammable material or atmosphere and an ignition source. Ordnance that is not contained could provide an ignition source. The point of installation into the containment device needs to be determined and evaluated for its potential as an ignition source. It is expected that the ordnance will be fully assembled prior to receipt by the satellite organization.

This analysis will only address ordnance upon receipt at the point of installation. The manufacturers of the ordnance will be responsible for safety during the manufacturing, handling and transportation to the government destination.

The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments; they are all self-contained in their housings. Ordnance are usually installed during prelaunch services either at the hazardous processing facility or at the launch pad.

A band clamp type separation system is currently being proposed for COLD-SAT. This system has frangible bolts that are self-contained and will not produce high energy fragments or contamination.

## HAZARD DEFINITIONS

5. ; G.

How can Propulsion cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.G.1.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. The standard facility safety requirements and systems will be relied upon to control site modifications. Under normal site modification operations propulsion components would not be present at or in the vicinity of the facility being modified.</li></ul>
5.G.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. COLD-SAT will use a Centaur upper stage for delivery to orbit and will use a hydrazine reaction control system for propulsive attitude control. The subsystem manufacturers will have approved system safety plans to assure that safety is considered during manufacturing of subsystem testing.</li></ul>
5.G.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. The propulsion system will not normally be charged during transportation. If there is a need to transport a charged N2H4 system, system safety and applicable transportation and handling regulations will be addressed in the transportation procedures.</li></ul>
5.G.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. The propulsion system will not normally be charged during element assembly. If there is a need to charge the system with a propellant during element assembly, system safety will assure that the appropriate safeguards are in place to assure safe operations.</li></ul>
5.G.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. A system safety authority will approve all element test plans. All potential fire hazards relating to propulsion will be addressed in the test plans or site safety plans.</li></ul>
5.G.6.1 (system integration)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. The propulsion system will not be charged during system integration. If the system has been previously charged, system safety will verify by procedure review and approval that the system has been properly been flushed/vented/sealed, prior to handling during system integration.</li></ul>
5.G.7.1 (system test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. If any system tests are required on the propulsion system, they are normally performed using a flammable medium. A system safety authority will review and approve all procedures/plans and will assure that adequate safeguards are in place to prevent fires.</li></ul>

- 5.G.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. The hydrazine system is normally charged during prelaunch services and adequate safeguards need to be designed into the propulsion to eliminate the risk of fire.
- 5.G.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The hydrazine system will be charged during countdown and adequate safeguards need to be designed into the propulsion system to eliminate the risk of fire.
- 5.G.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. The pyrotechnic valves that isolate the N2H4 from the REMs needs to be fired some time after lift-off. If hydrazine leaked and if there is enough oxidizer present to produce a flammable mixture and an ignition source, a fire could occur. The design needs to incorporate safeguards to prevent a hydrazine leak.
- 5.G.11.1 (flight phase II) - No design impact during feasibility study. A propellant leak would not cause a fire in the vacuum of space. The propellant must be contained, be mixed with an oxidizer and have an ignition source to occur.
- 5.G.12.1 (payload separation) - No design impact during feasibility study. A propellant leak would not cause a fire in the vacuum of space. The propellant must be contained, be mixed with an oxidizer and have an ignition source to occur.

Author's notes: How can Propulsion cause Fire during \_\_\_\_\_ Operational Phase?

The hydrazine and any cleaning solvents that are used for the propulsive attitude control system and could cause fire hazards are addressed 5.B., hazardous materials cause fire.

## **HAZARD DEFINITIONS**

5. ; H.

**How can Non-Ionizing Radiation cause Fire during \_\_\_\_\_ Operational Phase?**

<b>CODE</b>	<b>DESCRIPTION</b>
-------------	--------------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how non-ionizing radiation can cause fire during any of the operational phases. Non-ionizing radiation is neither a ignition source nor will it support combustion and therefore is not a potential fire hazard.

Author's notes: How can Non-Ionizing Radiation cause Fire during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves. The level of non-ionizing radiation from the spacecraft antenna is very low and is very unlikely to cause injury to personnel. The communication GSE where high energy radio waves are used is not included in this analysis.

## HAZARD DEFINITIONS

5. ; I.

How can Ground Support Equipment cause Fire during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
5.I.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There are many ways that GSE could cause fire during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li> </ul>
5.I.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li> </ul>
5.I.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address the potential for fires caused by GSE will be included in the ground operations plan. These transportation plans will be reviewed and approved by a project safety authority.</li> </ul>
5.I.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. The potential for hazards will be reported to NASA via safety plans.</li> </ul>
5.I.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for fire caused by GSE during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</li> </ul>
5.I.6.1 (system integration)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for GSE causing fires, the safety engineer will assure that appropriate safety measures are known and in place.</li> </ul>

5.I.7.1 (system test)

- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for fire caused by GSE during system tests, the safety engineer will assure that appropriate safety measures are known and in place.

5.I.8.1 (prelaunch services)

- No design impact during feasibility study. The GSE designs are not developed to an adequate level to determine the potential for safety hazards. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

5.I.9.1 (countdown)

- No design impact during feasibility study. The GSE designs are not developed to an adequate level to determine the potential for safety hazards. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

5.I.10.1 (flight phase I)

+ Not applicable: this phase does not apply to the cause category/hazard group. GSE is not used after liftoff and therefore the potential for GSE causing fires is nonexistent.

5.I.11.1 (flight phase II)

+ Not applicable: this phase does not apply to the cause category/hazard group. GSE is not used after liftoff and therefore the potential for GSE causing fires is nonexistent.

5.I.12.1 (payload separation)

+ Not applicable: this phase does not apply to the cause category/hazard group. GSE is not used after liftoff and therefore the potential for GSE causing fires is nonexistent.

Author's notes: How can Ground Support Equipment cause Fire during \_\_\_\_\_ Operational Phase?

Fire is caused a combination of combustible material and an ignition source. GSE provides the potential for both, such as in the loading equipment for N2H4 and the LH2/GH2 storage and handling equipment. Ignition sources can be a spark from electrical equipment or an electrostatic discharge.



## HAZARD DEFINITIONS

6. ; A.

How can the Structural/Mechanical system cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.A.1.1	(launch site mods.)
6.A.2.1	(subsystem mfg.)
6.A.3.1	(transportation)
6.A.4.1	(element assembly)
6.A.5.1	(element test)

6.A.1.1 (launch site mods.)

- No design impact for feasibility study. Occurrences such as a pressure vessel receiving structural/mechanical damage could cause an explosion/implosion. There could be pressure vessels at the launch site during modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.

6.A.2.1 (subsystem mfg.)

- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.

6.A.3.1 (transportation)

- No design impact for feasibility study. Structural/mechanical damage that could result in an explosion/implosion of pressure vessels is very likely to occur during transportation. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. This will include adequate protective devices. Safety considerations that will address the potential for an explosion/implosion caused by structural/mechanical damage will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.

6.A.4.1 (element assembly)

- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When there is the potential for an explosion/implosion resulting from structural/mechanical damage during element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to reduce the hazardous condition to an acceptable level. The potential for hazards will be reported to NASA via safety plans.

6.A.5.1 (element test)

- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for an explosion/implosion resulting from structural/mechanical damage during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.

- 6.A.6.1 (system integration) - No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for an explosion/implosion resulting from structural/mechanical damage, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.A.7.1 (system test) - No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for an explosion/implosion resulting from structural/mechanical damage, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.A.8.1 (prelaunch services) \* This could be a design impact and should be considered during preliminary design. There will be many pressure vessels used during prelaunch services that could explode/implode as a result of structural/mechanical damage. The pressures and time-lines as well as the potential for structural/mechanical damage need to be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, Chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 6.A.9.1 (countdown) - No design impact during feasibility study. Pressures can be increased as high as MEOP during countdown. If a pressure vessel has sustained prior structural/mechanical damage, the potential for an explosion/implosion exists during countdown. Quality assurance and the process and test procedures will be relied upon to assure that structural/mechanical damage does not occur.
- 6.A.10.1 (flight phase I) - No design impact during feasibility study. Some pressures can be increased as high as MEOP during flight phase I due to systems being locked up and the loss of atmosphere. If a pressure vessel has sustained prior structural/mechanical damage the potential for an explosion/implosion exists during flight phase I. Quality assurance and the process and test procedures will be relied upon to assure that structural/mechanical damage does not occur.
- 6.A.11.1 (flight phase II) - No design impact during feasibility study. Some pressures can be increased as high as MEOP during flight phase II due to systems being locked up and the loss of atmosphere. If a pressure vessel has sustained prior structural/mechanical damage the potential for an explosion/implosion exists during flight phase II. Quality assurance and the process and test procedures will be relied upon to assure that structural/mechanical damage does not occur.

6.A.12.1.1 (payload separation) - No design impact during feasibility study. Some pressures can be increased as high as MEOP during payload separation due to systems being locked up and the loss of atmosphere. If a pressure vessel has sustained prior structural/mechanical damage the potential for an explosion/implosion exists during payload separation. Quality assurance and the process and test procedures will be relied upon to assure that structural/mechanical damage does not occur.

Author's notes: How can the Structural/Mechanical system cause an Explosion during \_\_\_\_\_ Operational Phase?

A pressure vessel that was structure weakened by mechanical/structural damage could result in the pressure vessel exploding/implosion. Potential situations that could cause structural/mechanical damage to pressure vessels need to be listed and considered for methods to eliminate their root causes. Structural/mechanical damage frequently occurs during handling, installation or when work is being performed in the local area. Procedures and quality control is normally relied upon to prevent structural/mechanical damage.

## HAZARD DEFINITIONS

6. ; B.

How can Hazardous Materials cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.B.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There are many ways that hazardous materials could cause explosions during launch site modifications such as welding or operating a cutting torch with cleaning or painting solvents in the area. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
6.B.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. It will be the responsibility of the manufacturers of the subsystems to assure the safety of the hardware and personnel, which includes explosions from hazardous materials. All subsystem manufacturers will be required to have a NASA approved safety plan, per their contract. The potential for using hazardous materials that could cause explosions will be identified during contract discussions.</li></ul>
6.B.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards that are associated with each material.</li></ul>
6.B.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When hazardous materials are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent explosions. The potential for hazards will be reported to NASA via safety plans.</li></ul>
6.B.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for the use of hazardous materials that could cause explosions. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. Upon determination that a test has potential for explosion from hazardous materials during the element tests, the system engineer will assure that appropriate safety measures are known and in place. An example is the testing of LH2 components.</li></ul>

- 6.B.6.1 (system integration)
- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all plans for potential safety impacts. Upon determination that a process has potential for an explosion of hazardous materials during system integration, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.B.7.1 (system test)
- \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. All system tests using LH2 need to be considered for methods to reduce their hazards during the feasibility study.
- 6.B.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. Items that might impact the preliminary design are the LH2 tanking/de-tanking; LH2 venting, N2H4 tanking/de-tanking; payload separation systems or arming the pyrotechnic devices.
- 6.B.9.1 (countdown)
- \* This could be a design impact that should be considered during preliminary design. Systems for the proper venting of GH2 during countdown may have a design impact and need to be considered during the preliminary design. The other hazardous materials need to be reviewed for potential design impacts.
- 6.B.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. During flight phase I, the greatest amount of stress and vibration will normally occur. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.
- 6.B.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

6.B.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. Payload separation involves a shock factor and an ignition source. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

Author's notes: How can Hazardous Materials cause an Explosion during \_\_\_\_\_ Operational Phase?

The shock could explode shock sensitive materials or combinations of materials. A shape charge type system might ignite a flammable mixture. The concepts proposed for feasibility study includes only pyrotechnics that are self-contained. The propulsion cause category, 6.G, will address the potential for propellants causing explosions.

Hazardous materials need to be controlled. They can be in a solid, liquid or gaseous state or a combination of these states. A project approved materials list will be compiled. It will include the hazards or hazardous conditions for each material that will be used on the project. The known hazardous materials that are currently associated with COLD-SAT are LH2/GH2, N2H4, components or by-products of batteries, or solvents used in processing. Methods for controlling these hazardous materials will be considered during the preliminary design phase of the program.

## HAZARD DEFINITIONS

6. ; C.

How can Environmental Conditions cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.C.1.1 (launch site mods.)	<p>- No design impact for feasibility study. At the feasibility study phase of the program, it can not be determined how environmental conditions could cause explosions/implosions during launch site modifications. System safety will analyze the design during each phase of the program to determine if there are any potential hazards associated with environmental conditions causing explosion/implosion.</p>
6.C.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements. These will include the potential for environmental conditions causing explosions/implosions.</p>
6.C.3.1 (transportation)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. A variety of environmental conditions will be encountered during transportation. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. These transportation plans will be reviewed and approved by a project safety authority.</p>
6.C.4.1 (element assembly)	<p>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When there are environmental conditions that provide the potential for explosions/implosions, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the hazard from occurring. The potential for hazards will be reported to NASA via safety plans.</p>

- 6.C.5.1.1 (element test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions to cause explosions/implosions during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.C.6.1 (system integration)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for environmental conditions causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.C.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for environmental conditions that provide the potential for explosions/implosions during the system tests, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.C.8.1 (prelaunch services)
- No design impact during feasibility study. There will be many adverse environmental conditions encountered during prelaunch services such as the MLI blanket purge and the LH2 tank verification tests. Excessive pressures or the extremely cold temperatures could contribute to the potential for an explosion/implosion.
- 6.C.9.1 (countdown)
- No design impact during feasibility study. There will be many adverse environmental conditions encountered during countdown, such as the MLI blanket purge and the LH2 tanking operation. Excessive pressures or the extremely cold temperatures could contribute to the potential for an explosion/implosion.
- 6.C.10.1 (flight phase I)
- No design impact during feasibility study. There will be many adverse environmental conditions encountered during flight, such as the MLI blanket evacuation, shock and vibrations. Pressure differentials or the extremely cold temperatures could contribute to the potential for an explosion/implosion.
- 6.C.11.1 (flight phase II)
- No design impact during feasibility study. There will be many adverse environmental conditions encountered during flight, such as the MLI blanket evacuation, shock and vibrations. Pressure differentials or the extremely cold temperatures could contribute to the potential for an explosion/implosion.



6.C.12.1.1 (payload separation) - No design impact during feasibility study. There will be many adverse environmental conditions encountered during payload separation, such as the space environment and the shock of the separation device. Pressure differentials or the extremely cold temperatures from the LH2 could contribute to the potential for an explosion/implosion.

Author's notes: How can Environmental Conditions cause an Explosion during \_\_\_\_\_ Operational Phase?

Explosion/implosion is a sudden or violent burst outward/inward. This violent burst may cause injury to personnel or damage to equipment. Environmental condition causing rapid heating or cooling could result in an explosion or implosion.

Environmental conditions are: shock/vibration; temperature extremes; uninhabitable atmospheres; excessive moisture (rain or condensation); salt air; lightning; ESD, (electrostatic discharge); etc.

Lightning strike causing an explosion or a contained explosive atmosphere and an ignition source are examples of environmental conditions that could cause explosion/implosion. Lightning protection is standard practice for all aerospace operations.

## HAZARD DEFINITIONS

6. ; D.

How can Pneumatics cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.D.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There are many ways that pneumatics could cause an explosion/implosion during launch site modifications. Pressurants or gas supplies are commonly contained in high pressure bottles and spheres. The standard facility safety requirements and systems will be relied upon to control operations during site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
6.D.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Pneumatics that will have the potential for explosions will be used through out the manufacturing process. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li></ul>
6.D.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Pneumatics will be used during transportation of the tanks and the assembled satellite which will have the potential for an explosion/implosion. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that address pneumatics that could cause explosions/implosions will be included in the transportation plans. These transportation plans will be reviewed and approved by a project safety authority.</li></ul>
6.D.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When assembly operations have the potential for pneumatics causing explosions/implosions, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to reduce the hazard to an acceptable level. The potential for hazards will be reported to NASA via safety plans.</li></ul>

- 6.D.5.1 (element test)
- \* This could be a design impact and should be considered during preliminary design. There will be many element tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.D.6.1 (system integration)
- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.D.7.1 (system test)
- \* This could be a design impact and should be considered during preliminary design. There will be many system tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.D.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Pressure vessel design factors of safety and processing sequences need to be considered during the preliminary design of the satellite and GSE. Pneumatics, such as the GHe pressurants, will be used during the prelaunch services. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 6.D.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite and GSE need to have adequate factors of safety and verification testing to assure that they will withstand the countdown phase including any launch delays and abort situations.
- 6.D.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factors of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.

6.D.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factors of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.

6.D.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factors of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.

Author's notes: How can Pneumatics cause an Explosion during \_\_\_\_\_ Operational Phase?

## HAZARD DEFINITIONS

6. ; E.

How can the Electrical/Electronics system cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.E.1.1.1 (launch site mods.)	* This could be a design impact and should be considered during preliminary design. The launch site will require explosion proof electrical boxes on any level that may encounter LH2/GH2. This may require a major launch site modification to accommodate the handling of LH2/GH2.
6.E.2.1 (subsystem mfg.)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.
6.E.3.1 (transportation)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address the potential for electrical/electronics to cause an explosion during transportation will be included in the transportation plans.
6.E.4.1 (element assembly)	- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When electrical/electronics are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the explosion/implosion. The potential for hazards will be reported to NASA via safety plans.
6.E.5.1 (element test)	- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for the electrical/electronics system causing an explosion/implosion during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.

- 6.E.6.1 (system integration) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.E.7.1 (system test) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will evaluate the test plans for their potential of the electrical/electronics system causing an explosion/implosion and will assure that appropriate safety measures are known and in place to reduce the hazards to an acceptable level.
- 6.E.8.1 (prelaunch services) \* This could be a design impact and should be considered during preliminary design. There will be electrical/electronics in use during prelaunch servicing. All electrical/electronics that will be in use during prelaunch servicing will be evaluated by a system safety engineer to determine if it could be an ignition source for an explosive atmosphere. The responsible system safety engineer will assure appropriate safety measures are known and in place to reduce the hazards to an acceptable level.
- 6.E.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The LH2 boil-off will need to be diverted away from any ignition sources such as electrical/electronics that could provide an ignition source. The system safety engineer will evaluate the proposed designs to assure that there is adequate separation of the GH2 and any ignition sources.
- 6.E.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics providing ignition of any combustible atmosphere.
- 6.E.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics providing ignition of any combustible atmosphere.

6.E.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics providing ignition of any combustible atmosphere.

Author's notes: How can the Electrical/Electronics system cause an Explosion during \_\_\_\_\_ Operational Phase?

Electrical/electronics could be an ignition source for an explosion. An explosive atmosphere must also be present in order to cause a hazard. The LH2/GH2 environment, including the vents, provide an explosive atmosphere. The potential for hazardous materials, such as LH2/GH2, to cause explosion is addressed in 6.B.

## HAZARD DEFINITIONS

6. ; F.

How can Ordnance cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

6.F.1.1.1 (launch site mods.)	- No design impact during feasibility study. Ordnance is not typically included as part of launch site modifications. If ordnance are part of launch site modification, the site safety officer should be knowledgeable of their presence and take appropriate actions.
-------------------------------	---

6.F.2.1 (subsystem mfg.)	- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements.
--------------------------	---

6.F.3.1 (transportation)	- No design impact during feasibility study. The transportation of any ordnance device or component with an installed ordnance device will be controlled by applicable regulatory agencies and will require written procedures. These procedures will be reviewed and approved by the applicable regulatory agencies.
--------------------------	---

6.F.4.1 (element assembly)	- No design impact during feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be written into the procedures. Element assembly of ordnance devices will be performed by qualified personnel.
----------------------------	--

6.F.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test that involves ordnance has potential for explosion, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.
------------------------	---

6.F.6.1 (system integration)	- No design impact during feasibility study. Ordnance are not normally installed at integration. If there is a need to install ordnance at this point, system safety will review the justification and take appropriate actions. This information is not available at the feasibility study phase of this program.
------------------------------	--

6.F.7.1 (system test)	* This could be a design impact that should be considered during the preliminary design. There may be a need to test ordnance during system testing. The safety engineer needs to understand the impact of this testing and plan accordingly.
-----------------------	---



- 6.F.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. A project list for the desired pyrotechnic application needs to be compiled and the applications and installation sequence should be considered early in the design. System safety should be a primary contributor to this effort.
- 6.F.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.
- 6.F.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.
- 6.F.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.
- 6.F.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.

Author's notes: How can Ordnance cause an Explosion during \_\_\_\_\_ Operational Phase?

It is expected that the ordnance will be fully assembled prior to receipt by the satellite organization.

This analysis will only address ordnance upon receipt at the point of installation. The manufacturers of the ordnance will be responsible for safety during the manufacturing, handling and transportation to the government destination.

The concept proposed for feasibility study does not include any ordnance that has the potential to produce high energy fragments; they are all self-contained in their housings. Ordnance are usually installed during prelaunch services either at the hazardous processing facility or at the launch pad.

A band clamp type separation system is currently being proposed for COLD-SAT. This system has frangible bolts that are self-contained and will not produce high energy fragments or contamination.

## HAZARD DEFINITIONS

6. ; G.

How can Propulsion cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.G.1.1 (launch site mods.)	+ Not applicable: it currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during launch site modifications. Launch site modification that involve propulsion system GSE will be considered in 6.I, GSE causes Explosion/Implosion.
6.G.2.1 (subsystem mfg.)	+ Not applicable: it currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during subsystem manufacturing. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements.
6.G.3.1 (transportation)	+ Not applicable: it currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during transportation. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for each subassembly and major assembly will be stated in the requirements documentation. Safety considerations that will address the potential for the propulsion system to provide an ignition source for an explosive atmosphere will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.
6.G.4.1 (element assembly)	+ Not applicable: it currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during element assembly. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When there is a potential for the propulsion system to provide an ignition source for an explosive atmosphere, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent a hazardous conditions. The potential for hazards will be reported to NASA via safety plans.

- 6.G.5.1 (element test)
- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for to provide an ignition source for an explosive atmosphere, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.G.6.1 (system integration)
- No design impact during feasibility study. It currently can not be conceived how the propulsion system can contribute to an explosion during system integration. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that an integration process provides the potential for the propulsion system to provide an ignition source, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.G.7.1 (system test)
- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test provides the potential for the propulsion system to provide an ignition source for an explosion, the safety engineer will assure that appropriate safety measures are known and in place.
- 6.G.8.1 (prelaunch services)
- No design impact during feasibility study. It currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during prelaunch services. During tanking of the hydrazine, the current design has an pyro-isolation valve between the N2H4 bottles and the thrusters and the thruster valves provide an additional barrier. The standard procedure for tanking hydrazine includes sampling the atmosphere for the presence of any hazardous gases.
- 6.G.9.1 (countdown)
- No design impact during feasibility study. It currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during countdown. The propulsion system will be sealed during countdown.
- 6.G.10.1 (flight phase I)
- No design impact during feasibility study. It currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during the flight phase. The pyro-isolation valve will be activated soon after launch and will supply N2H4 to the thruster valves. The proposed valves have dual seats to provide a redundant seal.
- 6.G.11.1 (flight phase II)
- No design impact during feasibility study. It currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during the flight phase. The pyro-isolation valve will be activated soon after launch and will supply N2H4 to the thruster valves. The proposed valves have dual seats to provide a redundant seal.

6.G.12.1.1 (payload separation) - No design impact during feasibility study. It currently can not be conceived how the propulsion system could provide an ignition source that could cause an explosion during payload separation. The pyro-isolation valve will be activated soon after launch and will supply N2H4 to the thruster valves. The proposed valves have dual seats to provide a redundant seal.

Author's notes: How can Propulsion cause an Explosion during \_\_\_\_\_ Operational Phase?

Propulsion could cause explosions by providing an ignition source to an explosive environment or the propellant could provide the explosive environment. Block 6.B, Hazardous Materials cause Explosion addresses the potential for the hydrazine to provide an explosive atmosphere. The propulsive system will be activated after payload separation. Some elements of the propulsive system may be activated during testing. This analysis will consider any potential for the propulsive system to provide an ignition source for an explosive environment.

## HAZARD DEFINITIONS

6. ; H.

How can Non-Ionizing Radiation cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

This cause category/hazard group does not apply to COLD-SAT.

Currently, it can not be conceived how Non-ionizing radiation can cause Explosion/Implosion during any of the operational phases.

Author's notes: How can Non-Ionizing Radiation cause an Explosion during \_\_\_\_\_ Operational Phase?

Non-ionizing radiation is generated by high energy radio waves. The prevailing hazard is injury to personnel from exposure to the energy of the waves. The energy of the waves is not sufficient to cause structural damage to equipment that would normally be used on or around a satellite. If the energy from the radiation was absorbed by the medium contained in a pressure vessel, an over-pressure condition could result. All GSE and flight systems that are associated with the satellite will be protected against over-pressure conditions. That condition requires a second order failure and therefore it is addressed as a first order hazard elsewhere in this hazard analysis. The communication GSE where high energy radio waves are used is not included in this analysis.

## HAZARD DEFINITIONS

6. ; I.

How can Ground Support Equipment cause an Explosion during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
6.I.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System safety will evaluate all GSE that provides a pressure differential to determine the potential for explosion or implosion.</li></ul>
6.I.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. It currently can not be conceived how the GSE can cause an explosion/implosion during subsystem manufacturing.</li></ul>
6.I.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The transportation requirements for the major elements of GSE will be stated in the requirements documentation. Safety considerations that will address potential for explosion/implosion hazard will be included in the transportation plan. These transportation plans will be reviewed and approved by a project safety authority.</li></ul>
6.I.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The GSE will be manufactured per engineering requirements that will be adequate to endure the anticipated pressures. System safety will evaluate the designs to assure that all safety requirements will be satisfied.</li></ul>
6.I.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing of major GSE. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for GSE to contribute to an explosion during the element tests, the safety engineer will assure that appropriate safety measures are known and in place.</li></ul>

6.I.6.1 (system integration) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that an integration process has potential for GSE to contribute to an explosion/implosion, the safety engineer will assure that appropriate safety measures are known and in place.

6.I.7.1 (system test) - No design impact during feasibility study. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for GSE to contribute to the potential for an explosion/implosion, the safety engineer will assure that appropriate safety measures are known and in place.

6.I.8.1 (prelaunch services) \* This could be a design impact and should be considered during preliminary design. The handling of LH2 during prelaunch services could provide an opportunity for an explosion/implosion. System safety will evaluate the equipment designs and servicing operations to determine the potential for an explosion/implosion.

6.I.9.1 (countdown) \* This could be a design impact and should be considered during preliminary design. GSE may be required for maintaining pressures in the LH2 tank during countdown. System safety will evaluate the equipment designs and operations to determine the potential for an explosion/implosion.

6.I.10.1 (flight phase I) + Not applicable: this phase does not apply to the cause category/hazard group.

6.I.11.1 (flight phase II) + Not applicable: this phase does not apply to the cause category/hazard group.

6.I.12.1 (payload separation) + Not applicable: this phase does not apply to the cause category/hazard group.

Author's notes: How can Ground Support Equipment cause an Explosion during \_\_\_\_\_ Operational Phase?

Explosion/implosion is a sudden or violent burst outward/inward. This violent burst may cause injury to personnel or damage to equipment.

An explosion can result from an over-pressure condition that exceeds the structural capabilities of a containment device. An implosion is the same conditions except the pressures are reversed. Any of the GSE that provides a pressure differential needs to be evaluated for explosion or implosion.

## HAZARD DEFINITIONS

### 7. ; A.

How can the Structural/Mechanical system cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
------	-------------

Currently, it can not be conceived how Structural/Mechanical failures could cause Temperature Extremes.  
All condition that the author has postulated are addressed in other Hazard Group/Cause Categories.

Author's notes: How can the Structural/Mechanical system cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

Temperature extreme hazards resulting from the release of hazardous materials due to structural/mechanical failures are second order effects and are addressed as first order effects in 7.B, Hazardous materials causing temperature extremes.



## HAZARD DEFINITIONS

7. ; B.

How can Hazardous Materials cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.B.1.1 (launch site mods.)	<p>- No design impact for feasibility study. Currently, it can not be conceived how the hazardous materials that are associated with launch site modifications could cause temperature extremes. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</p>
7.B.2.1 (subsystem mfg.)	<p>- No design impact for feasibility study. The program safety requirements will be stated in the contract and will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements and will include hazardous materials and their potential for causing temperature extremes.</p>
7.B.3.1 (transportation)	<p>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazardous materials that could cause temperature extremes.</p>
7.B.4.1 (element assembly)	<p>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When hazardous materials that could cause temperature extremes are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent injury or damage. The potential for hazards will be reported to NASA via safety plans.</p>
7.B.5.1 (element test)	<p>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test may involve hazardous materials that could cause temperature extremes during the element tests, the safety authority will assure that appropriate safety measures are known and in place.</p>

- 7.B.6.1 (system integration)
- No design impact during feasibility study. Currently, it can not be conceived how the hazardous materials that are associated with system integration could cause temperature extremes. System integration will be accomplished via procedures and plans. System safety will consider all system integration operations for potential safety impacts. Upon determination that a process may include hazardous materials that could cause temperature extremes, the safety authority will assure that appropriate safety measures are known and in place.
- 7.B.7.1 (system test)
- No design impact during feasibility study. There is a high probability that LH2/GH2 will be used during system testing. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test may include hazardous materials that could cause temperature extremes, the safety engineer will assure that appropriate safety measures are known and in place.
- 7.B.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. LH2/GH2, GHe and N2H4 will be loaded during prelaunch services. These hazardous materials could cause temperature extreme hazards. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.
- 7.B.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and create a hazardous condition (e.g. leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition).
- 7.B.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and create a hazardous condition (e.g. leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition).
- 7.B.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and create a hazardous condition (e.g. leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition).

7.B.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and create a hazardous condition (e.g. leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition).

Author's notes: How can Hazardous Materials cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

If hydrazine contacts oxides and other materials that it reacts with, a rapid heating, i.e. a temperature extreme, would result. When pressurants are loaded, a rapid fill rate can cause an over-heating of the medium and the system. The cryogenic temperatures of LH2 classifies it as hazardous material that can cause severe injury to personnel and structural damage. When high pressure gases are released, the friction of the escaping gas could cause a temperature extreme.

## HAZARD DEFINITIONS

7. ; C.

How can Environmental conditions cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.C.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
7.C.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The program safety requirements will be stated in the contracts which will require that the subsystem manufacturers have a qualified/approved safety program. Their program will address system and facility safety requirements.</li></ul>
7.C.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The transportation of major subassembly and assembly will be required to have written plans/procedures. These transportation plans will be reviewed and approved by a project safety authority. Environmental conditions causing temperature extremes will be considered during that review.</li></ul>
7.C.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When environmental conditions have the potential for causing temperature extremes, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the hazardous effects. The potential for hazards will be reported to NASA via safety plans.</li></ul>
7.C.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for an environmental condition that could cause temperature extremes during the element tests, the safety authority will assure that appropriate safety measures are known and in place. It is very likely that cold gas or cryogenics will be used during element testing.</li></ul>

- 7.C.6.1 (system integration)
- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all tests for potential safety impacts. Upon determination that an environment condition has potential for temperature extremes during system integration, the safety engineer will assure that appropriate safety measures are known and in place.
- 7.C.7.1 (system test)
- No design impact during feasibility study. Test plans/procedures will be required for all system testing. System safety will consider all tests for potential safety impacts. Upon determination that a test has potential for an environmental condition that could cause temperature extremes during the system tests, the safety engineer will assure that appropriate safety measures are known and in place. It is very likely that cold gas or cryogenics will be used during system testing.
- 7.C.8.1 (prelaunch services)
- \* This could be a design impact and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. There is the potential for temperature extremes from cold gas purging. Human presence should not be required during cold gas purging.
- 7.C.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes on equipment and operations, such as cold gas purges and cryogenics, will be considered during the preliminary design. Where possible, the design will eliminate potential for hazards.
- 7.C.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes on equipment and operations, such as cold gas purges and cryogenics, will be considered during the preliminary design. Where possible, the design will eliminate potential for hazards.
- 7.C.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes on equipment and operations, such as cold gas purges and cryogenics, will be considered during the preliminary design. Where possible, the design will eliminate potential for hazards.

7.C.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes on equipment and operations, such as cold gas purges and cryogenics, will be considered during the preliminary design. Where possible, the design will eliminate potential for hazards.

Author's notes: How can Environmental conditions cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

The environment is any area or condition in an area. Temperature extreme is any temperature, either hot or cold, that is beyond what could be considered normal for the item that it is effecting. For humans, a temperature extreme is something that could cause burns or freezing of flesh. For equipment, an extreme is the temperature that could cause a malfunction. A cold gas environment could cause freezing of humans while cryogenic temperatures may render electronic or mechanical components inoperable.

The hazards associated with cryogenics causing temperature extremes is addressed by 7.B, Hazardous Materials causing Temperature Extremes.

## HAZARD DEFINITIONS

7. ; D.

How can Pneumatics cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.D.1.1 (launch site mods.)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. During site modifications involving pneumatic systems the standard facility safety requirements and systems will be relied upon for control, including the requirements of ESMCR 127-1, chapter 5.</li></ul>
7.D.2.1 (subsystem mfg.)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements including any potential for pneumatics causing temperature extremes that would create a safety hazard.</li></ul>
7.D.3.1 (transportation)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards that are associated with each material including the hazards of pneumatics causing temperature extremes.</li></ul>
7.D.4.1 (element assembly)	<ul style="list-style-type: none"><li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When pneumatics that could cause temperature extremes are to be used in an element assembly, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to reduce the hazard to an acceptable level. The potential for hazards will be reported to NASA via safety plans.</li></ul>
7.D.5.1 (element test)	<ul style="list-style-type: none"><li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for the use of pneumatics that could cause temperature extremes. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. Upon determination that a test has potential for temperature extremes from hazardous materials during the element tests, the system engineer will assure that appropriate safety measures are known and in place. An example is the testing of cryogenic components using cold gases.</li></ul>

- 7.D.6.1 (system integration) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.
- 7.D.7.1 (system test) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.
- 7.D.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic storage, supply and discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.
- 7.D.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.
- 7.D.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.
- 7.D.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.
- 7.D.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.

Authors note's: How can Pneumatics cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

Pneumatics can cause temperature extremes from using cold pressurants or rapidly escaping high pressure gases. The temperature extremes could cause critical components to malfunction.



## HAZARD DEFINITIONS

7. ; E.

How can the Electrical/Electronics system cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.E.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There are many ways that the electrical/electronics system can cause temperature extremes during launch site modifications. The standard facility safety requirements and systems will be relied upon to control site modifications, including the requirements of ESMCR 127-1, chapter 5.</li> </ul>
7.E.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. The manufacturers of electrical/electronic equipment will be required to have a NASA approved system safety plan. It will be the responsibility of the subsystem manufacturers to assure the safety of their personnel, including the hazards associated with temperature extremes of electrical/electronic equipment.</li> </ul>
7.E.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Any transportation of electronics/electronics, either as components, assemblies, or after integration, will be considered during the design for the potential of temperature extremes. In cases where the hazards can not be eliminated or reduced to an acceptable level, proper handling will be controlled by the procedures.</li> </ul>
7.E.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies will be considered by a safety engineer and appropriate safety controls will be included in the procedures. When the potential for temperature extremes is evident, it will be the responsibility of the organization that is performing the operation to assure that there are adequate controls to prevent the potential hazards. The potential for hazards will be reported to NASA via safety plans.</li> </ul>
7.E.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that there is a potential for temperature extreme hazards during an element test, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.</li> </ul>
7.E.6.1 (system integration)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. During system integration there will be many operations concerning the electrical/electronics system. The preliminary design should consider the integration methods and reduce the potential for temperature extremes in the design.</li> </ul>

7.E.7.1 (system test)

\* This could be a design impact that should be considered during the preliminary design. There is a potential for the electrical/electronics system causing temperature extremes during system testing because the systems will have power applied to them. The system engineer will consider the locations and accessibility of electrical/electronics for their potential effect on other components or injury to personnel.

7.E.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. There is a potential for the electrical/electronics system causing temperature extremes during prelaunch services because the systems will have power applied to them. The system engineer will consider the locations and accessibility of electrical/electronics for their potential effect on other components or injury to personnel.

7.E.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.

7.E.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.

7.E.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.

7.E.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.

Author's notes: How can the Electrical/Electronics system cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

Electrical/Electronics can cause temperature extremes by normal heating during use, by over-heating during use due to an anomaly, or by an external heat source. The temperature extremes can render critical components inoperable or cause injury to personnel.

## HAZARD DEFINITIONS

7. ; F.

How can Ordnance cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.F.1.1.1 (launch site mods.)	- No design impact during feasibility study. Ordnance is not typically included as part of launch site modifications. If ordnance are part of launch site modification, the site safety officer should be knowledgeable of their presence and take appropriate actions.
7.F.2.1 (subsystem mfg.)	- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements.
7.F.3.1 (transportation)	- No design impact during feasibility study. The transportation of any ordnance device or component with an installed ordnance device will be controlled by applicable regulatory agencies and will require written procedures. These procedures will be reviewed and approved by the applicable regulatory agencies.
7.F.4.1 (element assembly)	- No design impact during feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be written into the procedures. Element assembly of ordnance devices will be performed by qualified personnel.
7.F.5.1 (element test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test that involves ordnance has potential for temperature extremes, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.
7.F.6.1 (system integration)	- No design impact during feasibility study. Ordnance are not normally installed at integration. If there is a need to install ordnance at this point, system safety will review the justification and take appropriate actions.
7.F.7.1 (system test)	- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test that involves ordnance has potential for temperature extremes, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.

- 7.F.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. A project list of the desired pyrotechnic application and locations will to be compiled during the preliminary design. System safety will be a primary contributor to this effort and will evaluate the potential for temperature extremes at that time.
- 7.F.9.1 (countdown) \* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.
- 7.F.10.1 (flight phase I) \* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.
- 7.F.11.1 (flight phase II) \* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.
- 7.F.12.1 (payload separation) \* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.

Author's notes: How can Ordnance cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

Ordnance causing fire and explosion are addressed in 5.F and 6.F respectively. Temperature extremes may render critical components inoperable or cause injury to humans that contact the ordnance device soon after activation. Under normal conditions, the ordnance devices will only be activated during testing and in use. Tests will be controlled by test plans which will include the appropriate safety measures. When ordnance are activated in use, it will be during countdown or after launch and therefore humans will not be present. For normal activation system safety will only be concerned with temperature extremes rendering critical components inoperable. The inadvertent activation of ordnance devices is a concern. The preliminary design will consider the power requirements for activation and the necessary inhibits that are required to prevent inadvertent activation.

## HAZARD DEFINITIONS

7. ; G.

How can Propulsion cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.G.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Propulsion systems are not a part of the launch site and therefore are not a hazard concern. The hazards associated with the GSE that supports the propulsion system are addressed in cause category I, GSE.</li> </ul>
7.G.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements. Any potential for propulsion causing temperature extremes will be considered by the appropriate safety authority at the subsystem manufacturers.</li> </ul>
7.G.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The Department of Transportation and state and local regulations control the transportation of hazardous materials. A system safety authority will approve procedures that include the transportation of hazardous materials. The "program hazardous materials list" will be used to identify the hazards that are associated with each material.</li> </ul>
7.G.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Assembly procedures will be written and used for all assemblies. All assemblies that may have a safety impact will be considered by a safety engineer and appropriate safety controls will be written into the procedures. Element assembly of ordnance devices will be performed by qualified personnel.</li> </ul>
7.G.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. Test plans/procedures will be required for all testing. System safety will consider all tests for potential safety impacts. Upon determination that a test that has the potential for propulsion causing temperature extremes, the system engineer will assure that appropriate safety measures are activated to reduce the hazard to an acceptable level.</li> </ul>
7.G.6.1 (system integration)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. System integration will be accomplished via procedures and plans. System safety will consider all procedures for potential safety impacts. Upon determination that a procedure or process has potential for propulsion causing temperature extremes during system integration, the system safety authority will assure that appropriate safety measures are known and included in the process.</li> </ul>

- 7.G.7.1 (system test)
- \* This could be a design impact that should be considered during the preliminary design. There may be a need to test the propulsion system during system testing. The project safety engineer needs to understand the impact of this testing and plan accordingly.
- 7.G.8.1 (prelaunch services)
- \* This could be a design impact that should be considered during the preliminary design. The potential for the propulsion system causing temperature extremes during prelaunch servicing and its impact needs to be reviewed by the project safety engineer.
- 7.G.9.1 (countdown)
- \* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during countdown.
- 7.G.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during flight phase I.
- 7.G.11.1 (flight phase II)
- \* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during flight phase II.
- 7.G.12.1 (payload separation)
- \* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during payload separation.

Author's notes: How can Propulsion cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

Propulsion includes any system that has the potential for causing propulsion; it is not restricted to the propulsion system.

## HAZARD DEFINITIONS

7. ; H.

How can Non-Ionizing Radiation cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.H.1.1 (launch site mods.)	- No design impact during feasibility study. There should be no use of non-ionizing radiation during launch site modifications.
7.H.2.1 (subsystem mfg.)	- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements. Any potential for non-ionizing radiation will be considered by the appropriate safety authority at the subsystem manufacturers. The manufacturers should include interlocks and shielding in the designs of RF equipment. The safety engineer will assure that these are included in the equipment.
7.H.3.1 (transportation)	- No design impact during feasibility study. The equipment must be under power to be a hazard. Under normal operating conditions, equipment is not under power when it is being transported.
7.H.4.1 (element assembly)	- No design impact during feasibility study. The element assemblies will be performed using procedures. System safety will consider all assemblies for their non-ionizing hazard potential.
7.H.5.1 (element test)	- No design impact during feasibility study. There will be a potential for non-ionizing radiation during element testing. System safety will be included in the element testing of non-ionizing equipment to determine potential hazards and will assure adequate safeguards have been incorporated.
7.H.6.1 (system integration)	* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes, such as interlocks and shielding, should be considered during the preliminary design.
7.H.7.1 (system test)	* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes, such as interlocks and shielding, should be considered during the preliminary design.

- 7.H.8.1 (prelaunch services) \* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes, such as interlocks and shielding, should be considered during the preliminary design.
- 7.H.9.1 (countdown)
- No design impact during feasibility study. Normally, any satellite equipment that could cause non-ionizing radiation is not active during countdown.
- 7.H.10.1 (flight phase I)
- No design impact during feasibility study. Normally, any satellite equipment that could cause non-ionizing radiation is not active during flight phase I.
- 7.H.11.1 (flight phase II)
- No design impact during feasibility study. Normally, any satellite equipment that could cause non-ionizing radiation is not active during flight phase II.
- 7.H.12.1 (payload separation)
- No design impact during feasibility study. There is not any potential hazards involving non-ionizing radiation causing temperature extremes during payload separation.

Author's notes: How can Non-Ionizing Radiation cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

The GSE communication equipment is not included in this analysis. Non-ionizing radiation may be a concern during testing of the flight systems. There is potential for non-ionizing radiation during use or anytime systems have power applied.



## HAZARD DEFINITIONS

7. ; I.

How can Ground Support Equipment cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

CODE	DESCRIPTION
7.I.1.1 (launch site mods.)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. There are many operations that will cause temperature extremes during site modifications, such as welding. The standard facility safety requirements and existing systems will be relied upon to control hazards during site modifications, including the requirements of ESMCR 127-1, chapter 5.</li> </ul>
7.I.2.1 (subsystem mfg.)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. The program safety requirements will be stated in the contract and will require the subsystem manufacturers to have a qualified/approved safety program. Their program will address system and facility safety requirements. The manufacturing or modification of GSE that might involve temperature extremes will be the responsibility of the subsystem manufacturers.</li> </ul>
7.I.3.1 (transportation)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. (How can GSE cause Temperature Extremes during transportation?)</li> </ul>
7.I.4.1 (element assembly)	<ul style="list-style-type: none"> <li>- No design impact during feasibility study. The organization that is responsible for GSE element assembly will also be responsible for assuring that temperature extremes are not a potential hazard. These operation may be performed at the manufacturer or at remote locations. The safety authority who is responsible for the facility will assure that safe operations are performed there.</li> </ul>
7.I.5.1 (element test)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. Testing of GSE will be performed in accordance with test plans/procedures. The appropriate system safety authority will assure that the potential for temperature extremes are addressed to reduce the hazards to an acceptable level. This includes the potential for cold as well as hot items.</li> </ul>
7.I.6.1 (system integration)	<ul style="list-style-type: none"> <li>- No design impact for feasibility study. The appropriate system safety authority will assure that the potential for temperature extremes are addressed to reduce the hazards to an acceptable level during system integration of the GSE.</li> </ul>

7.I.7.1 (system test)

- No design impact for feasibility study. System level testing will be performed using test plans/procedures. The appropriate system safety authority will assure that the potential for temperature extremes are addressed to reduce the hazards to an acceptable level. The GSE used to load/unload the LH2 may be tested using LH2 or cold GH2.

7.I.8.1 (prelaunch services)

- No design impact for feasibility study. Procedures for the use of GSE will be used for all operations. The area safety authority will review all procedures to assure that the potential for hazards is reduced to an acceptable level.

7.I.9.1 (countdown)

- No design impact for feasibility study. Procedures for the use of GSE will be used for all operations. The area safety authority will review all procedures to assure that the potential for hazards is reduced to an acceptable level.

7.I.10.1 (flight phase I)

- No design impact for feasibility study. The GSE used during flight phase I is limited to equipment used for telemetry.

7.I.11.1 (flight phase II)

- No design impact for feasibility study. The GSE used during flight phase II is limited to equipment used for telemetry.

7.I.12.1 (payload separation)

- No design impact for feasibility study. The GSE used during payload separation is limited to equipment used for telemetry.

Author's notes: How can Ground Support Equipment cause Temperature Extremes during \_\_\_\_\_ Operational Phase?

The potential for burns from the extraterrestrial communication equipment is addressed by 7.H.

## APPENDIX A2

### Classifications

## Major Safety Concerns from COLD-SAT Hazard Analysis

### COLLISION/MECHANICAL

- 1.A.9.1 (countdown)
- \* This could be a design impact that should be considered during preliminary design. Any component on the spacecraft or associated GSE could cause damage if it failed during countdown. The safety engineer would rely on adequate designs, testing and QA to assure that failures will not occur. The potential hazards are that the failure goes undetected and the launch occurs. Therefore it is critical that there are enough detection methods to alert the launch team to these failures.
- 1.A.10.1 (flight phase I)
- \* This could be a design impact that should be considered during the preliminary design. During flight phase I the greatest amount of stress and vibration will normally occur. Any of the satellite components could fail mechanically or structurally and cause collision or mechanical damage. In addition, the nose fairing or its components could fail and impact the satellite. The system safety engineer must rely on adequate design, testing and QA to assure that failures will not occur. If a failure occurs during flight phase I, there is no option for evasive or corrective actions.

### ELECTRICAL SHOCK

- 4.I.1.1 (launch site mods.)

- \* This could be a design impacts and should be considered during preliminary design. There is insufficient design detail at the feasibility study phase of the program to analyze for safety impacts. The launch site is considered GSE and there will be many uses of electrical power on the launch site. System safety will evaluate the proposed launch site modifications during preliminary design to determine the potential for electrical shock/shorts during any operations.

### EXPLOSION

- 6.D.5.1 (element test)

- \* This could be a design impacts and should be considered during preliminary design. There will be many element tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determining that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.

- 6.D.7.1 (system test)

- \* This could be a design impacts and should be considered during preliminary design. There will be many system tests requiring pneumatics that have the potential for causing explosions/implosions. Test plans/procedures will be required for all testing. Design factors of safety need to be considered during the preliminary design of the pressure vessels that will be included on the satellite. System safety will consider all tests for potential safety impacts. Upon determining that a test has potential for pneumatics causing explosions/implosions, the safety engineer will assure that appropriate safety measures are known and in place.

- 6.E.1.1 (launch site mods.)

- \* This could be a design impacts and should be considered during preliminary design. The launch site will require explosion proof electrical boxes on any level that may encounter LH2/GH2. This may require a major launch site modification to accommodate the handling of LH2/GH2.

- 6.F.8.1 (prelaunch services)

- \* This could be a design impact that should be considered during the preliminary design. A project list for the desired pyrotechnic application needs to be compiled and the applications and installation sequence should be considered early in the design. System safety should be a primary contributor to this effort.

## Major Safety Concerns from COLD-SAT Hazard Analysis

### EXPLOSION (con't)

6.F.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.

6.F.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.

6.F.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.

6.F.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The sequence of ordnance activation needs to be considered early in the design to assure an adequate supply of power and to evaluate if the ordnance firing will impact other functions.

## Major Safety Concerns (partially addressed) from COLD-SAT Hazard Analysis

---

### FIRE

#### 5.D.8.1 (prelaunch services)

- \* This could be a design impacts and should be considered during preliminary design. GH2 is to be loaded prior to launch. This will require all electrical service in the area to be terminated or have only spark proof electrical components in use during GH2 loading. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

### EXPLOSION

#### 6.A.8.1 (prelaunch services)

- \* This could be a design impacts and should be considered during preliminary design. There will be many pressure vessels used during prelaunch services that could explode/implode as a result of structural/mechanical damage. The pressures and time-lines as well as the potential for structural/mechanical damage need to be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### COLLISION/MECHANICAL

1.A.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-safety approved procedures. (example of non-mission unique safety consideration: Personnel platforms structurally fail causing injury to personnel of damage to the satellite; example of a mission unique safety consideration: The LH2 supply line support brackets fracture resulting in damage to the line.)

1.G.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Re-contact after separation could occur if a RCS thruster fired upon or after separation. The RCS system needs to be designed to withstand the shock of separation without allowing N2H4 to leak onto the catalyst bed.

### CORROSION

2.B.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during prelaunch services. Design methods will be identified to reduce the impact of these hazards.

2.B.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during countdown. Design methods will be identified to reduce the impact of these hazards. Normally corrosion is a time related (slow) process which would not occur during the ground processing through payload separation phases.

2.B.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during launch phase I. Design methods will be identified to reduce the impact of these hazards. Normally corrosion is a time related (slow) process which would not occur during the ground processing through satellite end of life.

2.B.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during launch phase II. Design methods will be identified to reduce the impact of these hazards. Normally corrosion is a time related (slow) process which would not occur during the ground processing through satellite end of life.

2.B.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. System safety will review the "program hazardous materials list" and determine the potential for corrosion during payload separation. Design methods will be identified to reduce the impact of these hazards. Normally corrosion is a time related (slow) process which would not occur during the ground processing through satellite end of life.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### CORROSION (cont)

- |          |                      |  |
|----------|----------------------|--|
| 2.C.8.1  | (prelaunch services) | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. Many systems will be opened and exposed to the environment that could introduce elements of corrosion during prelaunch servicing. These operations need to be performed by experienced personnel and require adherence to approved procedures. The equipment designs need to include safeguards to prevent the introduction of contaminants during prelaunch services. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.</li> </ul> |
| 2.D.9.1  | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement, will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.</li> </ul>  |
| 2.D.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement, will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.</li> </ul>  |
| 2.D.11.1 | (flight phase II)    | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement, will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.</li> </ul>  |
| 2.D.12.1 | (payload separation) | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement, will be considered during the preliminary design and proper materials can be considered for those areas of concern. The project approved materials and processing list will control the potential for pneumatics causing corrosion.</li> </ul>  |

### CONTAMINATION

- |         |                      |   |
|---------|----------------------|---|
| 3.C.8.1 | (prelaunch services) | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. Many systems will be opened and exposed to the environment during prelaunch servicing. These operations need to be performed by experienced personnel and require adherence to approved procedures. The equipment designs need to include safeguards to prevent the introduction of contaminants during prelaunch services. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.</li> </ul> |
| 3.C.9.1 | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of environmental conditions during countdown, such as filling the LH2 tank and the cold gas purge in the nose fairing. Contamination could be introduced through any of the environmental condition. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.</li> </ul>   |



## Minor Safety Concerns from COLD-SAT Hazard Analysis

### CONTAMINATION (con't)

3.C.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as the G-loading, shock and vibrations or depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.

3.C.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as the G-loading, shock and vibrations or depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.

3.C.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The satellite will be exposed to a variety of stressful environmental conditions during flight, such as the G-loading, shock and vibrations or depressurization. These stressful conditions could cause particles/items to dislodge and contaminate the satellite. The contamination could result in a potential hazard. System safety will be an active participant of the design team so the potential hazards will be identified and eliminated early in the design.

3.D.6.1 (system integration)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.7.1 (system test)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.D.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. Pneumatics could contaminate the systems that it supplies causing components to be inoperable and creating a safety hazard. Clean pneumatic systems and proper filtering and contaminate detection methods should be considered during the preliminary design.

3.E.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. Prelaunch servicing will require electrical/electronics to be installed/removed which could provide an opportunity for contamination. The impact of the contamination will be evaluated by the program system safety authority for their potential safety hazards. Upon determining that there is a potential safety impact, the system safety authority will assure that the appropriate safety measures are incorporated.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### CONTAMINATION (cont)

- |          |                      |  |
|----------|----------------------|--|
| 3.E.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Depressurization upon ascent could cause out gassing resulting in contamination. The project approved materials list will indicate materials that have the potential for out gassing. System safety will verify that there are adequate design requirements to preclude out gassing that could result in a potential hazard.</li> </ul>                  |
| 3.E.11.1 | (flight phase II)    | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Depressurization upon ascent could cause out gassing resulting in contamination. The project approved materials list will indicate materials that have the potential for out gassing. System safety will verify that there are adequate design requirements to preclude out gassing that could result in a potential hazard.</li> </ul>                  |
| 3.F.8.1  | (prelaunch services) | <ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. Ordnance will be included in prelaunch servicing operations. When specifying the type of ordnance during the design phases the handling and installation methods need to be considered for their safety impacts. System safety will assist in determining proper methods for handling, installing and arming ordnance during prelaunch servicing.</li> </ul> |
| 3.G.8.1  | (prelaunch services) | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The hydrazine will be loaded during prelaunch servicing which provides an opportunity for the system to become contaminated. This contamination could be a potential safety hazard. The preliminary design should include adequate filters in the loading and on-board systems.</li> </ul>   |

### ELECTRICAL SHOCK

- |          |                      |   |
|----------|----------------------|---|
| 4.C.9.1  | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. LH2 is being tanked during countdown which creates the potential for temperature extremes and condensation. The preliminary design should consider the effects of these conditions on the electrical equipment.</li> </ul>                                    |
| 4.C.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The most severe shock and vibration conditions and liquid air run-off conditions occur at flight phase I. These conditions need to be considered in the design phase of development and methods to prevent electrical shock need to be considered.</li> </ul> |
| 4.C.11.1 | (flight phase II)    | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Very severe shock and vibration conditions and liquid air run-off conditions occur at flight phase II. These conditions need to be considered in the design phase of development and methods to prevent electrical shock need to be considered.</li> </ul>    |
| 4.C.12.1 | (payload separation) | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The separation system creates a shock when it is activated and need to be considered during the preliminary design for its potential for creating electrical shock.</li> </ul>  |
| 4.E.6.1  | (system integration) | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. During system integration there will be many operations concerning electrical/electronics. The preliminary design should consider the integration methods and reduce the potential for electrical shock in the design.</li> </ul>                             |

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### ELECTRICAL SHOCK (con't)

4.E.7.1 (system test)

\* This could be a design impact that should be considered during the preliminary design. During system testing there will be many opportunities for electrical shock from electrical/electronics. The preliminary design should consider testing methods and reduce the potential for electrical shock in the design.

4.E.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. During prelaunch services there will be many opportunities for electrical shock from electrical/electronics. The preliminary design should consider servicing methods and reduce the potential for electrical shock in the design.

4.E.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. During flight phase I, the greatest amount of stress and vibration will normally occur. The designers should consider the flight loads when specifying the electrical/electronics so they will be robust enough to withstand the launch environments.

4.E.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. During flight phase II a significant amount of stress and vibration will occur. The designers should consider the flight loads when specifying the electrical/electronics so they will be robust enough to withstand the launch environments.

4.E.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. There are some unique shock loads encountered during payload separation. The system designer needs to consider these loads and their effects of specific electronics/electrical components during preliminary design so that the risk of electrical shocks/shorts can be minimized.

4.F.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Ordnance will be installed and possibly armed during prelaunch services. The potential for electrical shocks or shorts will be evaluated by the system safety engineer during preliminary design and the system safety engineer will work with the design engineers to incorporate the appropriate design features to reduce the potential hazard to an acceptable level.

4.F.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The ordnance may be armed during countdown. Procedures will be used for all operations during countdown and system safety will review all procedures to identify any potential safety impacts. The potential for other hazards concerning ordnance and electrical shocks or shorts will be evaluated by the system safety engineer.

4.I.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. GSE will be used extensively during prelaunch servicing. System safety will evaluate the GSE and its use during prelaunch servicing to determine any potential for electrical shocks or shorts.

4.I.9.1 (countdown)

\* This could be a design impacts and should be considered during preliminary design. GSE will be used extensively during countdown. System safety will evaluate the GSE and its use during countdown to determine any potential for electrical shocks or shorts.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### FIRE

- |          |                      |   |
|----------|----------------------|---|
| 5.B.9.1  | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during preliminary design. Systems for the proper venting of GH2 during countdown may have a design impact and need to be considered during the preliminary design. The other hazardous materials that have the potential for causing fire need to be reviewed for potential design impacts.</li> </ul>  |
| 5.B.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. During flight phase I the greatest amount of stress and vibration will normally occur. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.</li> </ul> |
| 5.B.11.1 | (flight phase II)    | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.</li> </ul>  |
| 5.B.12.1 | (payload separation) | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Payload separation involves a shock factor and an ignition source. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.</li> </ul>                     |
| 5.D.9.1  | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during countdown. If the GH2 were to leak, it could be ignited by an electrical source of other operations during countdown.</li> </ul>  |
| 5.D.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by an electrical source of other flight operations.</li> </ul>   |
| 5.D.11.1 | (flight phase II)    | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by an electrical source of other flight operations.</li> </ul>   |
| 5.D.12.1 | (payload separation) | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. GH2 used for pneumatics will be contained on the satellite during flight. If the GH2 were to leak, it could be ignited by the shape charge or an electrical source during payload separation.</li> </ul>  |
| 5.E.9.1  | (countdown)          | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.</li> </ul>   |
| 5.E.10.1 | (flight phase I)     | <ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.</li> </ul>   |

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### FIRE (con't)

5.E.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.

5.E.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Proper containment of electrical/electronics and proper venting of GH2 will be considered during the preliminary design.

5.G.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. The hydrazine system is normally charged during prelaunch services and adequate safeguards need to be designed into the propulsion to eliminate the risk of fire.

5.G.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The hydrazine system will be charged during countdown and adequate safeguards need to be designed into the propulsion system to eliminate the risk of fire.

### EXPLOSION

6.B.9.1 (countdown)

\* This could be a design impact that should be considered during preliminary design. Systems for the proper venting of GH2 during countdown may have a design impact and need to be considered during the preliminary design. The other hazardous materials need to be reviewed for potential design impacts.

6.B.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. During flight phase I the greatest amount of stress and vibration will normally occur. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

6.B.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

6.B.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Payload separation involves a shock factor and an ignition source. The "program hazardous materials list" will be used to identify the hazards that are associated with each material. LH2 pressure control and venting methods need to be studied during the preliminary design for their potential safety impacts.

6.D.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite and GSE need to have adequate factor of safety and verification testing to assure that they will withstand the countdown phase including any launch delays and abort situations.

6.D.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factor of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### EXPLOSION (cont)

6.D.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factor of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.</li> </ul>
6.D.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Pressure vessels and relief systems on board the satellite need to have adequate factor of safety and verification testing to assure that they will withstand the launch loads and on-orbit environments.</li> </ul>
6.E.8.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. There will be electrical/electronics in use during prelaunch servicing. All electrical/electronics that will be in use during prelaunch servicing will be evaluated by system safety to determine if it could be an ignition source for an explosive atmosphere. The responsible system safety engineer will assure appropriate safety measures are known and are in place to reduce the hazards to an acceptable level.</li> </ul>
6.E.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The LH2 boil-off will need to be diverted away from any ignition sources such as electrical/electronics that could provide an ignition source. The system safety engineer will evaluate the proposed designs to assure that there is adequate separation of the GH2 and any ignition sources.</li> </ul>
6.E.10.1	(flight phase I)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics to provide an ignition of any combustible atmosphere.</li> </ul>
6.E.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics to provide an ignition of any combustible atmosphere.</li> </ul>
6.E.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. Any operations scheduled during ascent will be evaluated by the system safety engineer for the potential of electrical/electronics to provide an ignition of any combustible atmosphere.</li> </ul>
6.F.7.1	(system test)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. There may be a need to test ordnance during system testing. The safety engineer needs to understand the impact of this testing and plan accordingly.</li> </ul>
6.I.8.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. The handling of LH2 during prelaunch services could provide an opportunity for explosion / implosion. System safety will evaluate the equipment designs and servicing operations to determine the potential for explosion / implosion.</li> </ul>
6.I.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impacts and should be considered during preliminary design. GSE may be required for maintaining pressures in the LH2 tank during countdown. System safety will evaluate the equipment designs and operations to determine the potential for explosion/implosion.</li> </ul>

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### TEMPERATURE EXTREMES

7.B.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and creation a hazardous condition. (For example: Leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition.)

7.B.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and creation a hazardous condition. (For example: Leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition.)

7.B.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and creation a hazardous condition. (For example: Leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition.)

7.B.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. Hazardous materials could cause temperature extremes that could impact the operations of systems or components and creation a hazardous condition. (For example: Leaking LH2 could cool the satellite's or launch vehicle's instrumentation and cause an anomalous condition.)

7.C.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes, such as cold gas purges and cryogenics, on equipment and operations will be considered during the preliminary design. Where possible the design will eliminate potential for hazards.

7.C.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes, such as cold gas purges and cryogenics, on equipment and operations will be considered during the preliminary design. Where possible the design will eliminate potential for hazards.

7.C.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes, such as cold gas purges and cryogenics, on equipment and operations will be considered during the preliminary design. Where possible the design will eliminate potential for hazards.

7.C.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The effects of environmental conditions that might cause temperature extremes, such as cold gas purges and cryogenics, on equipment and operations will be considered during the preliminary design. Where possible the design will eliminate potential for hazards.

7.D.6.1 (system integration)

\* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.

7.D.7.1 (system test)

\* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### TEMPERATURE EXTREMES (con't)

7.D.8.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of pneumatic storage, supply and discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes. Also the potential for injury to personnel from pneumatic temperature extremes will be considered.</li> </ul>
7.D.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.</li> </ul>
7.D.10.1	(flight phase I)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.</li> </ul>
7.D.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.</li> </ul>
7.D.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of pneumatic discharge or vents will be considered for their impingement on critical items that could be effected by temperature extremes.</li> </ul>
7.E.6.1	(system integration)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. During system integration there will be many operations concerning electrical/electronics. The preliminary design should consider the integration methods and reduce the potential for temperature extremes in the design.</li> </ul>
7.E.7.1	(system test)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. There is a potential for electrical/electronics causing temperature extremes during system testing because the systems will have power applied to them. The system engineer will consider the locations and accessibility of electrical/electronics for their potential effect on other components or injury to personnel.</li> </ul>
7.E.8.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. There is a potential for electrical/electronics causing temperature extremes during prelaunch services because the systems will have power applied to them. The system engineer will consider the locations and accessibility of electrical/electronics for their potential effect on other components or injury to personnel.</li> </ul>
7.E.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.</li> </ul>
7.E.10.1	(flight phase I)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.</li> </ul>
7.E.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.</li> </ul>



## Minor Safety Concerns from COLD-SAT Hazard Analysis

### TEMPERATURE EXTREMES (con't)

7.E.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of equipment and its power-up time will be considered for potential temperature extreme hazards.</li> </ul>
7.F.8.1.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. A project list of the desired pyrotechnic application and locations will need to be compiled during the preliminary design. System safety will be a primary contributor to this effort and will evaluate the potential for temperature extremes at that time.</li> </ul>
7.F.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.</li> </ul>
7.F.10.1	(flight phase I)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.</li> </ul>
7.F.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.</li> </ul>
7.F.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The location of the ordnance devices needs to be considered so that the heat resulting from firing will not render other components or systems inoperable.</li> </ul>
7.G.7.1	(system test)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. There may be a need to test the propulsion system during system testing. The project safety engineer needs to understand the impact of this testing and plan accordingly.</li> </ul>
7.G.8.1	(prelaunch services)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The potential for the propulsion system causing temperature extremes during prelaunch servicing and its impact needs to be reviewed by the project safety engineer.</li> </ul>
7.G.9.1	(countdown)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during countdown.</li> </ul>
7.G.10.1	(flight phase I)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during flight phase I.</li> </ul>
7.G.11.1	(flight phase II)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during flight phase II.</li> </ul>
7.G.12.1	(payload separation)	<ul style="list-style-type: none"> <li>* This could be a design impact that should be considered during the preliminary design. The propulsion system needs to include adequate inhibits in the design to prevent temperature extremes during payload separation.</li> </ul>

## Minor Safety Concerns from COLD-SAT Hazard Analysis

### TEMPERATURE EXTREMES (cont)

7.H.6.1	(system integration)	* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes such as interlocks and shielding should be considered during the preliminary design.
7.H.7.1	(system test)	* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes such as interlocks and shielding should be considered during the preliminary design.
7.H.8.1	(prelaunch services)	* This could be a design impact that should be considered during the preliminary design. Methods for reducing the potential for non-ionization radiation causing temperature extremes such as interlocks and shielding should be considered during the preliminary design.

## Minor Safety Concerns (partially addressed) from COLD-SAT Hazard Analysis

### CORROSION

2.D.1.1 (launch site mods.)

\* This could be a design impact that should be considered during the preliminary design. A hydrogen supply and loading system will be added to the launch site and hydrogen embrittlement is a potential problem during or after launch site modifications. The primary means of controlling hydrogen embrittlement is to use materials that are approved for use in hydrogen environments. The project approved materials list will be used to control material selections. The standard facility safety requirements and systems will be relied on to control site modifications. These include the requirements of ESMCR 127-1, chapter 5.

2.D.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. The potential for pneumatics causing corrosion such as hydrogen embrittlement, will be considered during the preliminary design and proper materials can be considered for those areas of concern. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

2.G.8.1 (prelaunch services)

\* This could be a design impact that should be considered during the preliminary design. The current design includes two barriers between the N2H4 supply and the catalyst beds of the REMs, which will be in effect during prelaunch servicing. The servicing equipment designs will need to be analyzed for its adherence to the pad/area safety requirements, such as those stated in ESMCR 127-1, chapter 5. The mission unique activities will be conducted via safety approved procedures.

2.G.9.1 (countdown)

\* This could be a design impact that should be considered during the preliminary design. The current design includes two barriers between the N2H4 supply and the catalyst beds of the REMs, which will be in effect during countdown. The operation performed during countdown concerning the propulsion system will need to be analyzed for the potential for propulsion to cause corrosion and for adherence to safety requirements, such as those stated in ESMCR 127-1, chapter 5.

2.G.10.1 (flight phase I)

\* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. The flight sequence needs to be evaluated for potential safety hazards.

2.G.11.1 (flight phase II)

\* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. The flight sequence needs to be evaluated for potential safety hazards.

2.G.12.1 (payload separation)

\* This could be a design impact that should be considered during the preliminary design. The current concept is to release the N2H4 into the thruster loop soon after lift off. With the N2H4 in the lines during payload separation there is the potential for a fault that would fire the REMs and initiate or cause corrosion. The flight sequence needs to be evaluated for potential safety hazards.

### CONTAMINATION

3.B.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. For mission unique activities that involve hazardous materials, the safety engineer will perform an evaluation to determine the potential for contamination. Upon determining the potential for a hazardous situation, the safety engineer will ensure that there are adequate controls in place to reduce the hazards to an acceptable level and will verify that they are effective.

## Minor Safety Concerns (partially addressed) from COLD-SAT Hazard Analysis

### CONTAMINATION (cont)

#### 3.B.9.1 (countdown)

- \* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. For mission unique activities that involve hazardous materials, the safety engineer will perform an evaluation to determine the potential for contamination. Upon determining the potential for a hazardous situation, the safety engineer will ensure that there are adequate controls in place to reduce the hazards to an acceptable level and will verify that they are effective.

#### 3.E.9.1 (countdown)

- \* This could be a design impact that should be considered during the preliminary design. During countdown the electrical/electronics on board the space craft will be exposed to controlled environmental purge which is a design parameter for the electrical/electronics equipment. The GSE electrical/electronics equipment will be exposed to adverse environments that will also be included in the design requirements. The project system safety engineer will evaluate the design requirements and the designs to assure that they are adequate to preclude any potential hazards from electrical/electronics being contaminated.

### FIRE

#### 5.B.7.1 (system test)

- \* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements, ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. All system tests using LH2/GH2 need to be considered for methods to reduce their hazards during the feasibility study.

#### 5.B.8.1 (prelaunch services)

- \* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. The primary hazardous material that has the potential for causing fire during prelaunch services is LH2/GH2.

#### 5.E.8.1 (prelaunch services)

- \* This could be a design impacts and should be considered during preliminary design. Electrical/electronics and LH2/GH2 will be present and in-use during prelaunch services. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

#### 5.G.10.1 (flight phase I)

- \* This could be a design impact that should be considered during the preliminary design. The pyrotechnic valves that isolate the N2H4 from the REMs need to be fired some time after lift-off. If hydrazine leaked and if there is enough oxidizer present to produce a flammable mixture and an ignition source, a fire could occur. The design needs to incorporate safeguards to prevent a hydrazine leak.

### EXPLOSION

#### 6.B.7.1 (system test)

- \* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. All system tests using LH2 need to be considered for methods to reduce their hazards during the feasibility study.

## Minor Safety Concerns (partially addressed) from COLD-SAT Hazard Analysis

### EXPLOSION (con't)

6.B.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. Items that might impact the preliminary design are the LH2 tanking/de-tanking; LH2 venting, N2H4 tanking/de-tanking; payload separation systems or arming the pyrotechnic devices.

6.D.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Pressure vessel design factors of safety and processing sequences need to be considered during the preliminary design of the satellite and GSE. Pneumatics, such as the GHe pressurants, will be used during the prelaunch services. Pad/area safety plans will address the non-mission unique safety requirements, ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

### TEMPERATURE EXTREMES

7.B.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. LH2/GH2, GHe and N2H4 will be loaded during prelaunch services. These hazardous materials could cause temperature extreme hazards. Pad/area safety plans will address the non-mission unique safety requirements, ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures.

7.C.8.1 (prelaunch services)

\* This could be a design impacts and should be considered during preliminary design. Pad/area safety plans will address the non-mission unique safety requirements; ESMCR 127-1, chapter 5 is applicable. The mission unique activities will be conducted via safety approved procedures. There is the potential for temperature extremes from cold gas purging. Human presence should not be required during cold gas purging.

## Safety Concerns from COLD-SAT Hazard Analysis Addressed During Feasibility Study

### COLLISION/MECHANICAL

- |         |                      |  |
|---------|----------------------|--|
| 1.G.8.1 | (prelaunch services) | • This could be a design impact that should be considered during the preliminary design. To satisfy the requirements of ESMCR 127-1, there must be two barriers between the N2H4 and the catalyst beds. These barriers (valves) must be included in the design.                      |
| 1.G.9.1 | (countdown)          | • This could be a design impact that should be considered during the preliminary design. To satisfy the requirements of ESMCR 127-1, there must be two barriers between the N2H4 and the catalyst beds until after lift off. These barriers (valves) must be included in the design. |



National Aeronautics and  
Space Administration

## Report Documentation Page

1. Report No. NASA CR-187042		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle COLD-SAT Feasibility Study Safety Analysis				5. Report Date January 1991	
				6. Performing Organization Code	
7. Author(s) Steven T. McHenry and James M. Yost				8. Performing Organization Report No. None	
				10. Work Unit No. 506-48	
9. Performing Organization Name and Address Analex Corporation 21775 Brookpark Road Fairview Park, Ohio 44126				11. Contract or Grant No. NAS3-25515	
				13. Type of Report and Period Covered Contractor Report Final	
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Lewis Research Center Cleveland, Ohio 44135-3191				14. Sponsoring Agency Code	
15. Supplementary Notes Project Manager, Robert G. Rohal, Office of Mission Safety and Assurance, NASA Lewis Research Center.					
16. Abstract <p>The Cryogenic On-orbit Liquid Depot—Storage, Acquisition and Transfer (COLD-SAT) satellite presents some unique safety issues. The feasibility study conducted at the NASA Lewis Research Center desired a systems safety program that would be involved from the initial design in order to eliminate and/or control the inherent hazards. Because of this, a hazards analysis method was needed that: (1) identified issues that needed to be addressed for a feasibility assessment; and (2) identified all potential hazards that would need to be controlled and/or eliminated during the detailed design phases. This report presents the developed analysis method as well as the results generated for the COLD-SAT system.</p>					
17. Key Words (Suggested by Author(s)) COLD-SAT; Systems safety; Cryogenics; ELV; Microgravity experiment design				18. Distribution Statement Unclassified—Unlimited Subject Category 18	
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of pages 177	
				22. Price* A09	







National Aeronautics and  
Space Administration

**Lewis Research Center**  
Cleveland, Ohio 44135

Official Business  
Penalty for Private Use \$300

**FOURTH CLASS MAIL**

**ADDRESS CORRECTION REQUESTED**



Postage and Fees Paid  
National Aeronautics and  
Space Administration  
NASA-451

**NASA**

---